Bachelor's Thesis (UAS)

Bachelor's Degree in Information Technology

Specialization: Information Technology

2013

He Haijian

Network Security Threats and Defense

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor's Thesis | Abstract00

Turku University of Applied Sciences

Information Technology | Internet Technology

August 2013| Number of Pages: 45

Instructor: Patric Granholm

He Haijian

Network Security Threats and Defense

As we are already into the 21st century our society heavily relies on the Internet in several fields such as economics, politics, military. With the increasing impact of internet on our daily lives, various security risks are brought about by system defects, hackers and so on, which greatly threaten stability of the network, incur significant financial loss economically, and, to the most extreme extent, even can be a threat to national security. Therefore, network security has become an important issue of paramount importance in the field of economics, politics, military and people's lives.

This thesis is structured as follows: it first presents the current situation of network security, for example, the various ways and forms of current common attacks are, which are the source threats brought to the network. Chapter three introduces two of the most common network attacks we usually encounter as well as the corresponding countermeasures against every specific type of DOS and man-in-the-middle attacks. Chapter four focuses on two effective defense technologies, firewall and intrusion detection systems. Chapter four and five discuss the properties and characteristics of these two technologies along with the relative deployments and models that serve different purposes and applications. The purpose of the thesis is to discuss the common network attacks and two defense technologies so as to provide clues and mitigations for the increase in the difficulty of intrusion as well as the dramatic improvement in network security with the use effective countermeasures when network attacks are launched.

KEYWORDS:

network security, attacks, threat, defense, countermeasures

Contents Page

1. Background **1**

2. Analysis of the current network security **1**

2.1 Characteristics of network security 2

2.2 The main factors affecting network security 3

2.3 Major forms of attack 3

2.4 Threats which network security encounters 4

3.Types of network attacks **5**

3.2 Classification of network attacks 5

3.3 Denial of Service Attack 7

3.3.1 The Reasons account for DOS attack 8

3.3.2 Types of DOS attack 9

3.4 SYN flood 9

3.5 Smurf attack 13

3.6 UDP flood attack 14

3.7 Ping of Death 14

3.8 Land attack 14

3.9 Man-in-the-Middle Attack 16

3.10 ARP Spoofing 17

3.11 DNS Spoofing 21

4. Network Security Defense Technology **24**

4.1 Firewall Technology 25

4.2 What is Firewall 25

4.3 Firewall Functions 26

4.4 Firewall Classification 27

4.5 Firewall Limitations 28

4.6 Firewall Architecture 29

4.7 Packet filtering firewall 29

4.8 Dual-Homed Host Firewall 30
4.9 Screened Host Firewall 32
4.10 Screened Subnet 33
5. Intrusion Detection System 34
5.1 What is Intrusion Detection System 35
5.2 IDS structure 35
5.3 IDS Classification 36
5.4 IDS Approaches 39
5.5 Expert System misuse Detection 42
5.6 State Transition Analysis Misuse Detection 43
6. Summary 43
References 44

List of Figures

Figure 3.1 Illustration of a DOS attack
Figure 3.2 Illustration of a DDOS attack
Figure 3.3 Illustration of a complete three way handshake
Figure 3.4 Illustration of a half open connection
Figure 3.5 Illustration of a SYN flood
Figure 3.6 Illustration of SYN proxy defense against SYN attack
Figure 3.7 Illustration Smurf attack
Figure 3.8 Illustration of a Man-in-the-Middle attack (self-made)
Figure 3.9 Illustration of how ARP protocol works(With modifications)
Figure 3.10 Illustration of ARP spoofing process(With modifications)
Figure 3.11 Illustration of how DNS protocol works(With modifications)
Figure 3.12 Example of a DNS spoofing attack
Figure 4.1 Example of a firewall(With modifications)

Figure 4.2 Example of a Packet filtering firewall

Figure 4.3 Example of a Dual-homed host firewall

Figure 4.4 Example of a Screened host firewall

Figure 4.5 Example of a IDS Structure(with modifications)

Figure 4.6 Example of a HIDS Deployment

Figure 4.7 Example of a NIDS Deployment

Figure 4.8 Example of a neural network-based anomaly detection model

1. Background

Network security involves two aspects: physical and logical security. By logical security, we usually mean information security, including information confidentiality, integration and availability, and the meaning of the network security is the extension of information security, which means that network security is the protection for confidentiality, integration and availability of network information. Most of the network security issues are raised for the reason that malicious people known as hackers, try to get benefit for their own good. The meaning of network security varies between different users, for the reason that the familiarity and requirement about the network are different from user to user. For example, from the point of view of an ordinary user, what he/she desires from the internet is simply that all his/her privacy and confidential information are in protection while being transferred. In other words, information will not be intercepted and modified; while for the network providers, besides sharing the same concerns as the ordinary users, they also have to take the damages from abrupt natural disasters, military attacks and so on into account, and ways to restore network communication when it is abnormal.

Essentially, network security consists of network system hardware, software and the safety of the information being transferred through the Internet, protecting it from accidental or malicious attacks. As a result, network security involves the issues of technology and management, which are integrated as a whole. Network security faces challenge from network invasion and attacks.

2. Analysis of network security

As stated in the Citi Bank report in June 2011, the webpage of the bank suffered a hacker attack resulting in the theft of two-hundred thousand users' credit cards and personal information including username, account, home address email etc. Most of the victims were from Northern America. According to the report, a hacker illegally intruded Citi Bank's computer system, browsed and copied about two hundred thousand users' personal information. Reported on September 20, 2011, Japanese military production enterprise Mitsubishi Heavy Industries with factories of submarine, missile production and nuclear power plant component production were under hacker's attack, which might lead to an information disclosure, making Japanese national defense industry the target of hackers for the first time. During the investigation of the poisoned servers and computers, it emerged that a long time had elapsed before the attack discovered. The types of virus applied in this single attack were up to fifty, including twenty-eight types found in a single victim computer (Xiongyue 2011).

2.1 Characteristics of Network security

Five characteristics of Network security (Russ & Greg & Ed & Ted & Matthew, 2003)

1. Confidentiality - To ensure only authorized users get access to data, meanwhile, other users are restricted.

   Confidentiality is classified into network transmission confidentiality and data storage confidentiality. Network transfer confidentiality is achieved by encryption on data being delivered; while data storage confidentiality depends on the implementation of the access control.

2. Integrity - Data is not subject to change without authorization, in other words, information is unmodified, un-damaged and not lost during storage and delivery. Generally speaking, data integration is completed by access control, data backup and redundancy.

3. Availability - It refers data that is accessible by authorized entity and use as necessary, that is whether to store or access the needed information when required. Under the circumstance of network, Denial of Service ,network-undermining and all other operations which make the network unavailable are considered attacks to availability.

4. Non-repudiation refers to the property, in the middle of data transmission, of undeniable of information transferred, which is neither subject of being copied.

   Digital signature technology is one of the most important solution to non-repudiation.

5. Controllability it refers to people's ability to control on the route of the transmission, scale and the content of the information.

2.2 The main factors affecting the network security

The threats that network are encountering are various, there are threats to the network information as well as those to the devices. In general, threats are mainly divided into three categories:

1. Unintentional mistakes from staff. For instance, security holes caused by operators' improper safety configuration， users' low awareness of security, imprudent choice of passwords, sharing one's own personal account with others, all of which will lead to the possibility of the network being exposed to threats.

2. Man-made malicious attacks. So far, these threats are the most harmful to network security. Opponents' attacks and computer crimes belong to this category. These attacks are further classified into two types: active attacks, which selectively undermine the validity and integrity of the information; while the second type is passive attacks, for the possession of the confidential information, obtained by the means of interception, stealing and interpretation without the interruption of the network operation. These two types of attacks equally pose an incredible threat to the network security, which contributes to the disclosure of the confidential data.

3. Network software vulnerabilities and backdoor. There exist vulnerabilities in every software. These defeats and vulnerabilities are the target for attack by the hackers. A good percentage of the network intrusions results from inadequate safety measures, for instance, failure in a timely action to fill the system holes. Furthermore, for the convenience of maintenance, programmers staff who work for software companies, the backdoor they configured for the software is also a potential threat, The systems are accessible to anyone once the backdoor is open, which is a threat to network security.

2.3 Major forms of attack

Of all the attacks launched to Internet, usually there exists six different forms:

1. Theft and undermining from the internal staff. For instance, either purposely or carelessly, disclosure or modification of the record and undermining of the network system by the internal staff.

2.Taking advantage of some insecurity factors of the TCP/IP protocol. A considerable amount of security vulnerabilities concur the worldwide prevalent TCP/IP protocol, to carry ARP spoofing and launch IP spoofing attacks, with forged packets, specified routing source.

3. Information interception. Within the scope the electromagnetic radiation, firstly, in such a way like installation of device for interception, afterwards, by analysis of data flow and other parameters, hackers are able to extract useful information from the interception.

4. Virus-related undermining. System crashes or overwhelming servers with large quantity of spams, which lead to degradation in data performance, are a consequence of virus' consumption of the bandwidth, blocking of the network and breaking down servers.

5. Unauthorized access. It refers to intruders illegally accessing internet resources without permissions which are supposed to be granted from proper authorizations. Unauthorized access mainly includes illegal users breaking into the network or system for the illegal operations.

2.4 Threats which network security encounters

1. Computer virus

Computer viruses, which are programmed with advanced skills, are especially designed to undermine the ordinary operation of the computer. At present, the number of computer viruses is as high as up to roughly one hundred fourteen thousand, and the trend is that it will continue to grow and vary in sorts. The routes of their transmission can be through a hard disk, email via the Internet as well as software downloading. Computer viruses do not exit independently. Instead, they are parasitic in other programs, The nature of their existence render them extremely destructive, simultaneously with the feature of being hidden, latent and infectious, therefore, some viruses take advantage of these features to avoid detection by users. As it is up to the predetermined condition of the virus designer while the infected machine is working, the virus will come into effect by slowing the affected host down, corrupting files, affecting display, and, to a worse extend, it results in damage of hardware, system crash etc.

2. Hacker attacks

Network hacking refers to illegal conduct carried out by attackers, through the Internet, including unauthorized access, damage and attacks launched to network users, A hacker's motivation determines how hazardous an attack would be, in some cases, merely a hacker's curiosity drive them to spy on the secrets and privacy of the users without undermining the computer system, which is not a great harm. However, some hackers, instead of being curious, are driven by protest, rage, revenge, in an illegal way, to intrude and distort target user's pages and contents. All of these acts intend to make a serious negative impact, forcing the network out of service or rendering it unavailable. Some hackers are engaged in malicious attacks and destruction in an intrusion to erase and destroy those data of most importance of the computer system. To the national security, hacker attacks might be performed in the way of theft of confidential information relevant to national defense, military and political affairs etc., whereas conducts like embezzling of bank account for the withdraw of deposit are illegal acts performed to individually person. To conclude, hacker attacks are a great threat to the computer network.

3. Spam

Generally, spam indiscriminately, to delivers emails to the user mailbox without their permissions. The overwhelming amount of spam takes up considerable network bandwidth, causing congestion to the server which consequently, leads to a deficiently running network. In addition, spam is also a mean of spreading malicious software such as computer viruses and Trojan horses.

Network security is threatened for various reasons. Above all, technical staff, not being sufficient in the awareness of the security and poor in professional knowledge management, fail to take actively appropriate measures and precautions against current or future threats. Secondly, organizations and departments in the computer network fail to establish a complete and sound

management system which accordingly results in circumstances that security system and security control measures do not succeed in being fully effective. Additionally, this might be a good opportunity for the attackers to collect sensitive and important information. Finally, there exists a wild range of hacker attacks, which are diverse and flexible in the way they are conducted. Nowadays the trend is computer hackers tend to combine virus techniques in their attacks, making them more threatening to the network.

3.Types of network attacks

Hacker attacks originate either from hacker's own benefit, or interest, or upgrade to an intelligence war As a fact, under the circumstance of the modern network, hacker attacks occur every minute and second. Therefore, we should understand what a network attack is. However, a network attack is not so an easy to launch as it is imagined, hackers have to go through plenty of steps and progress to achieve it. First, the effective implementation of network attacks necessitates a grasp of the relative primary knowledge. Then, a hacker has to select a certain technique, in other words, to choose an appropriate means of attack, and after that, a wise method and procedure to follow. After these considerations, a desired expectation is to be achieved. Network attack refers to the whole process of using network commands as well as dedicated software downloaded from the Internet or software programmed by the hackers themselves. Hackers take advantage of an existing weakness of network communication protocol (TCP/IP protocol currently in use), security vulnerabilities originated from misconfigurations, or intrinsic defects of the user's operation system an illegally, to intrude the local or remote user host system for the possession, modification and deletion of the user information and the attachment of harmful information such as Trojan horses to the user system.

3.2 Classification of network attacks

Common network attacks are divided into six categories, 1) Blocking attack, 2) Control attack, 3) Detection attack, 4) Deception attack, 5) Hole attack, 6) Destruction attack. As it can be seen there exist many different types of attacks, but, for attacks launched to the network, attackers rely on more than one type of attack. As a matter of fact, it is often the case that a combination of different attacks are performed, to achieve their goals. For example, if a hacker intends to attack a system, he/she will solely use a detection attack to first detect information, and then might take the destructive attack for destruction.

1. Blocking Attack

In an attempt to force a possession of resource channel, network connection and storage, blocking attack tend to crash the servers or deplete the resources for the purpose of making them out of service. DOS (Denial of Service) is a typical blocking attack where the affected server denies service to legitimate users, that is to say, after being hacked, any request from legitimate users will not be responded. Common methods to launch DOS are: TCP and SYN flooding, E-mail bombing, land attack etc.

2. Controlling Attack

It is an attack which aims to gain control of the target machine. Trojan horse, password attack, buffer overflow attack are the three most common controlling attack. Among them, buffer overflow attack, a frequently used technique, which, in the early stage, hackers make use of the software's defect buffer overflow. Now, in a more advanced way, rather than using the self-existent buffer overflow, hackers create buffer overflow by inventing some new techniques.

3. Detection Attack

Usually, a detection attack is a preparation for a hacker who is about to launch attacks. With it, a diversity of the target information can be collected. Detection attacks includes the scanning technique which is applied to collect information about the architecture, information system, version and type of the operation system etc. So to say, through a detection attack, hackers will have a basic view of the information system and, afterwards, hackers are able to select appropriate tools and measures for further invasion.

Now a more advanced network traceless information detection technology is being developed. Hackers intend to improve their capability of being hidden, and leave no trace of evidence when they launch attacks, in order to avoid any evidence against them.

4. Deception Attack

It mainly includes IP deception and false message attack. By cheating, IP deception gains sensitive information in the disguise of legitimate network host, for example, hackers fake an IP address that is trustworthy to system host, so as to launch attacks.

5. Hole Attack

Attacks are carried out to various holes of the network system detected by scanners. As previously, the detection attack above is the prerequisite. The hole attack is characterized in being fast in updating, as a result, it is still very difficult to detect this kind of attack by even the latest intrusion detection system.

6. Destruction Attack

Destruction attack refers to an attack that is implemented on the data and software of the target machine, for example, computer virus, logic bomb, etc.

3.3 Denial of Service Attack(DOS)

DOS(Denial of Service) and DDOS(Distributed Denial of Service) are malicious attacks which intend to slow down traffic flow or disabling the server by sending a large amount of requests to network. Unlike viruses and worms which can inflict do serious damage to computer system and database, DOS suspend the service, and, in the worst case, they to crash the network for a period of time. In particular, DDOS are extremely harmful, in normal circumstances because all those previously infected hosts will come into the hacker's control, and

subsequently, in union, the infected hosts in infection send out forged information to the server, resulting in an increase in illegitimate flow. As a consequence, an legitimate request fails to be responded.

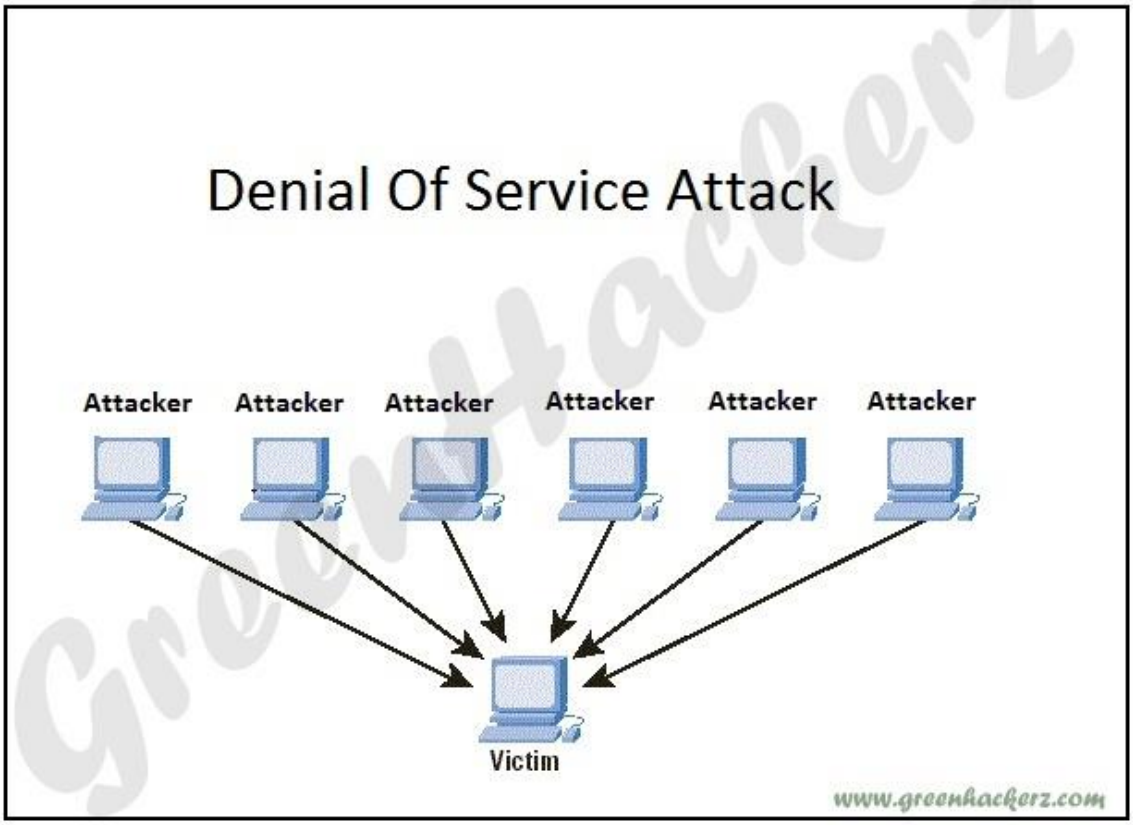

Figure 3.1 Illustration of a DOS attack

(http://www.google.com.hk)

First, the attacker sends a request with a forged IP address and the victim server answer it to that forged IP address Then, the server needs to receive an acknowledgement from the same IP address to finish this request, for the reason that IP address is forged, therefore, it will not issue an acknowledgement making the server to be in a state of waiting.

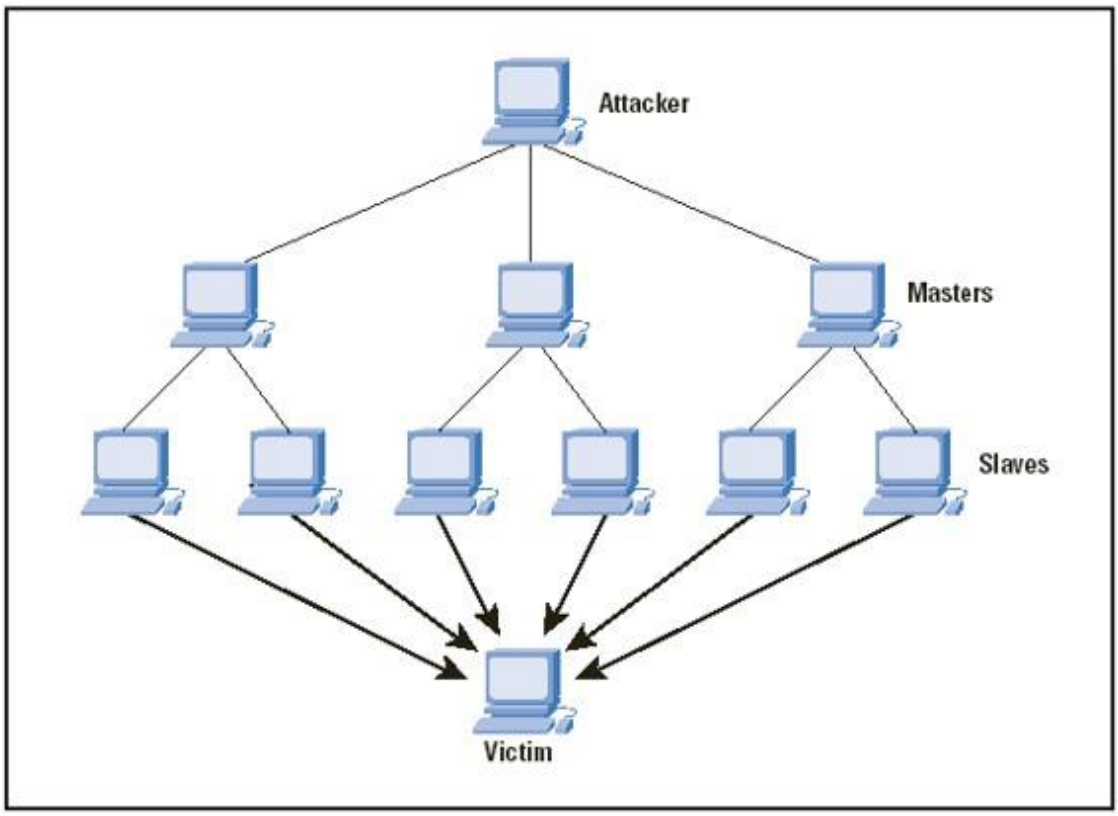

Figure 3.2 Illustration of a DDOS attack

(http://www.google.com.hk)

Attackers make the target hosts as a group that under his/her control making the hackers as masters of these victims hosts, all the slaves hosts will send remarkably large amount of requests to the victim host, making it to fail to provide services.

3.3.1 The Reasons account for DOS attack

DOS is an attack of can be found worldwide and millions of network users fall victims of this attack. Attackers are obsessed with its research, are professional in network and computer technology. By exploiting the vulnerabilities of the system and careful planning, hackers launch attacks after long preparation.

1 Misconfiguration

Quite often it is the case that configurations are done by administrators who have insufficient in experience and sense of responsibility. If the correct configuration is applied to the data storage, routers, firewall, switches of the network and other network-connected devices, the chances of being DOS attacked will be remarkably reduced.

2 Software vulnerability

For the reason that usually software are heavily dependent on the developers who are limited in the cost of design and short period in design and production, what is more, no software is perfect, as a result, vulnerabilities are inevitable. Being mal-programmed, while being attacked, the system builds an incessant process, using up the resources. Software vulnerabilities, generally, occur in the developers' failure in processing certain types of message or request while software is being developed. For this reason, when these types of massages are encountered during the operation of the software, it will turn to be abnormal, or even system.

3.3.2 Types of DOS attack

DOS attacks vary in types. The easiest one is launched by over-consumption of the service resources with reasonable service requests, resulting in service overload and other requests are not responded. Lack of resources, such as network bandwidth, file system space, opening process, which are caused by DOS attack is unavoidable no matter how fast the processing speed of the computer is, how large the memory capacity is and how board the bandwidth connected to the Internet is. Expectation of a high-efficient system for possessing high bandwidth and processing speed is wrong, because there exists a limit in any large capacity and a method in exceeding the maximum request value it is able to hold. As a consequence, DOS attacks will exhaust a tremendous resource.

3.4 SYN flood

SYN exploits TCP protocol defects, using up the resources of the victim by sending considerable amount of forged TCP requests. Among the common DOS attacks, SYN flood is the most popular and classical one.

There will be a three-way handshake when every single complete TCP request is generated from the user. First, a user originates a SYN message, then the service-provider answers with a SYN-ACK as acknowledgement after it has received the SYN, the user will respond by sending back an ACK after it has received the SYN-ACK from the server-host. Until this step, a complete three-

way handshake and a successful TCP connection are made as illustrated in the

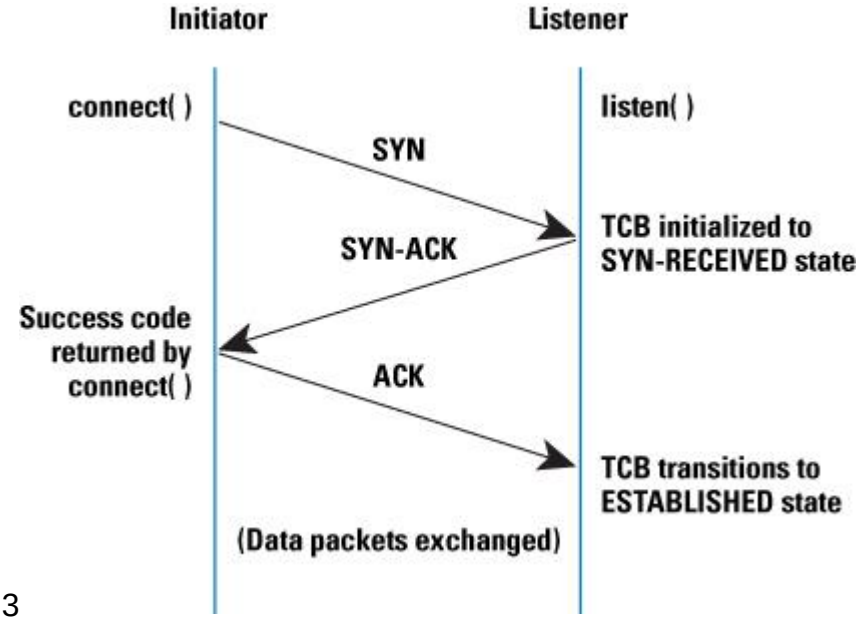

Figure 3.3

Figure 3.3 Illustration of a complete three way handshake

(http://www.google.com.hk)

During an TCP-SYN flood attack, only the first two steps are carried out. In other words, when the server-host receives a SYN-ACK message, by some means of deceit, the server will never receive ACK, as a result, it will be in a state of waiting for receiving the ACK message for a period of time, its technical term for this state is called “half-open connection”, as illustrated in Figure 3.4.

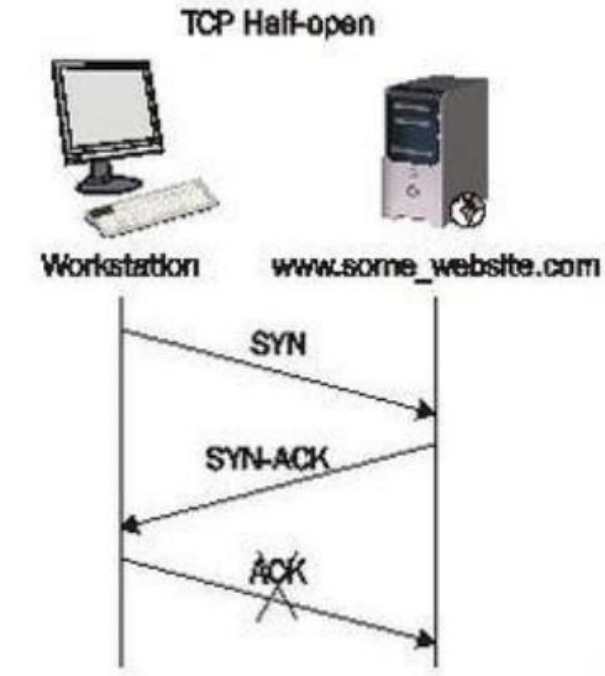

Figure 3.4 Illustration of a half open connection

(http://www.google.com.hk)

SYN flood takes advantage of the vulnerability of this three way handshake. Generally speaking, the victim is usually a server, for instance, a web server. Normally, attackers fake an unreachable source IP address, from which they generate a large quantity of TCP SYN packages. The TCP/IP protocol mechanism forwards a package solely based on the destination address without inspecting the validity of the source address. The victim server will respond to the source address, which is actually is forged and unreachable, when it receives the TCP SYN packages. Owing to the unreachability of the return path, the server is unable to make a successful TCP three way handshake and the connection to the attacker fails to establish, the server will again send SYN ACK to the client dropping the incomplete connection if it receives no response after waiting a certain period of time, which is a length of about thirty seconds to two minutes, which is called SYN timeout. Attackers continually repeat the SYN timeout by sending out overwhelming floods of SYN to the target server. As a consequence, there will be many incomplete half open connections, in the state of waiting in the queue of the victim server, which will be released until they are timeout. Because of the limited number of half open connections that is able to be accommodated by the server, the victim will not be capable of establishing any more new connections. When the maximum number of the half open connections is saturated, this results in the denial of service to legitimate users(Krawetz 2006).

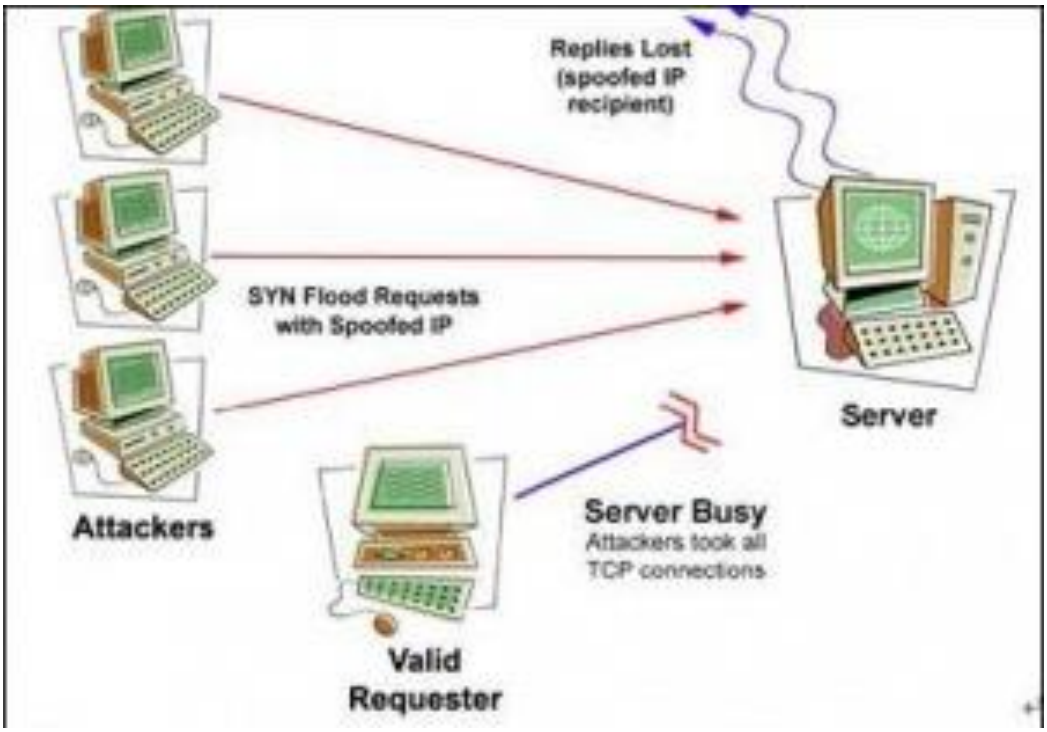

Figure 3.5 Illustration of a SYN flood

(http://www.google.com.hk)

SYN flood defense

For the SYN attack, if the administrator is familiar with the attacking mechanism and system structure, to a certain extent, he/she is able, through a series of measures, to mitigate the burden and negative influence brought by the attack. These measures include:

1) Cutting down the time takes to timeout

How much damage and effect that will inflicted to the victim is decided by the number of the SYN half open connections maintained by the target server, Suppose this value of damage is S, SYN attack frequency is F and timeout is T. S=F*T. To minimize the value of S, one way is to reduce the value of T, more specifically, that is to cut down the time it takes from the moment the server receives the SYN message to the moment confirming this message is invalid and drop that connection. For the defense of this attack, rather than the ordinary timeout duration of from thirty seconds to two minutes, a better choice would be less than twenty seconds, but not as short as possible for the reason that legitimate visitor accesses might be affected. According to the equation above, the impact performed on the victim depends on attack frequency and timeout, therefore, timeout-reducing is effective in the case of not very high attack frequency.

2) Routers

In a given of period of time, routers are able to play a role in permitting a limited number of half open connections, which, to a certain of extent, reduces the impact of the attack. For instance, one hundred is the maximum number of half open connections the server is able to hold, perhaps it is wise to restrict it to sixty, in this way, the cache of the target server will not be filled up when a SYN flood attack is launched.

3) SYN Proxy firewall

If the server does not establish a half open connection at the first handshake, instead, to establish a complete connection after receiving the third handshake, in this way, the resources of the server used for the establishment of the TCP connection will not be exhausted by the considerable amount of illegal first handshake packets, which are originated from the hosts. The working process of the SYN proxy is divided into three stages, the first stage is client's(Initiator's) three way handshake with the firewall(proxy), the difference with a usual three way handshake lies in, rather than directly with the server, the respondent is the firewall. The second stage: as a replacement for the client, the firewall generates a standard three-way handshake with the server(listener). The last stage: the sequence numbers and acknowledgement numbers are regulated and the connection is established. Only after these, the firewall will deliver the packet to the server, afterwards, the packet from the server is forwarded to the client. (SYN Flood Theory and Defense, 2012) as illustrated in Figure 3.6:

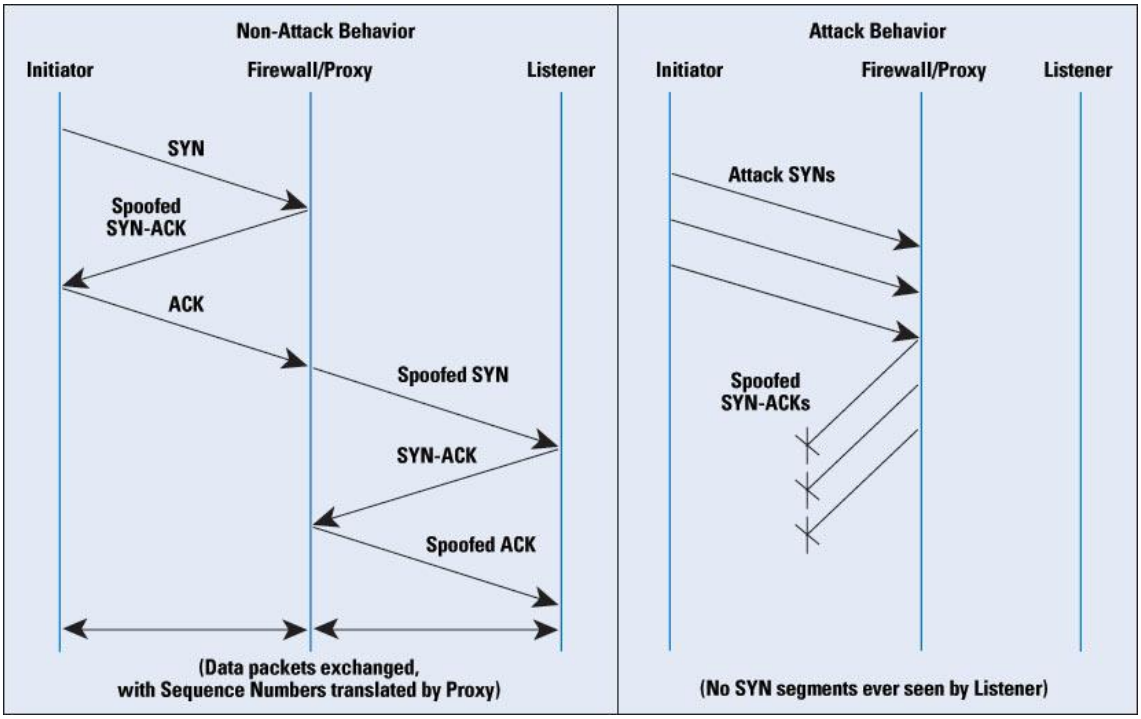

Figure 3.6 Illustration of SYN proxy defense against SYN attack

(http://blog.sina.com.cn/s/blog_4129523901013uuj.html)

As can be seen from Figure 3.6 in the left hand side, the firewall forwards the SYN request to the listener only after the connection is verified. On the right hand side, all the invalid connections are rejected by the firewall.

3.5 Smurf attack

Smurf is another form of DOS, which is an attack of great harm. The name of the attack is originates from the attacking program called “Smurf”. A smurf attack is composed of two parts: spoofed IP address and ICMP response.

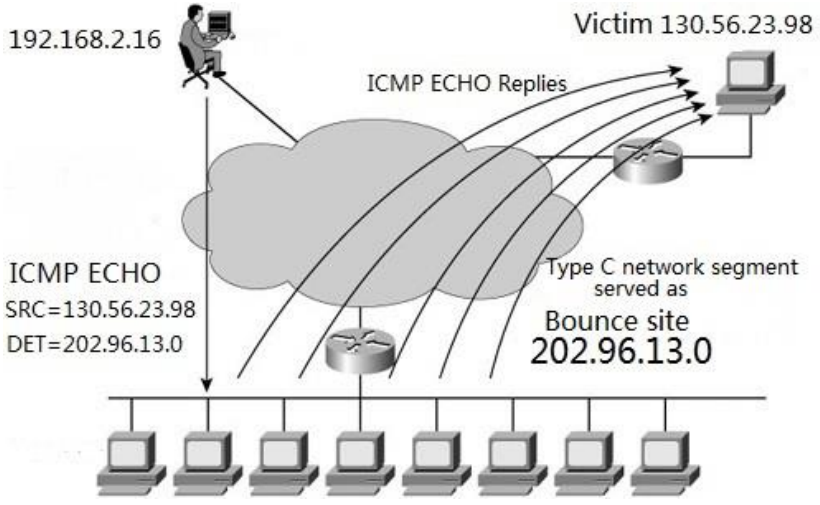

Figure 3.7 Illustration Smurf attack

(http://www.google.com.hk)

An attacker at IP address (192.168.2.16) pings another IP address, which will answer with an ICMP packet, on the condition that the corresponding host is available. If the destination of the ping from the attacker, instead of a IP address, is a broadcast address, for example (202.96.13.255), then after the network segment (202.96.13.0) receives that broadcast, all the hosts belong to the network segment will respond to attacker (192.168.2.16). In other words, every and each host will answer with an ICMP packet. The number of the packet, initiated from the attacker is one, but what he/she receives afterwards is 254 as much as sent, which is remarkably amplified, precisely, the number of the ICMP packet he/she receives is two hundred and fifty four, therefore, the network segment (202.96.13.0) functions as an ICMP amplifier which is called “Bounce site. However, in a usual case, this is not the way an attacker will behave, because all these ICMP packets will overwhelm him/herself, which is undesirable . Hence, the true purpose of the attack is to direct all these ICMP packets to the victim. Through some special hacking tool, the attackers fake his/her IP address (192.168.2.16) to that of the victim (130.56.23.98), so when the network segment (202.96.13.0) receives a broadcast ICMP packet, it will request all the hosts inside to answer to the source IP address where the ICMP packet came from. One vulnerability is that the network segment’s incapability to identify whether the source IP address is valid or not, as a result, all the respondent ICMP packets will forward directly to the victim (130.56.23.98).

If a network consists of a great amount of hosts, it will result in hundreds or thousands of respondents to the ECHO requests. Therefore, overwhelmed by the numerous ECHO RESPONSE packets, the target victim will not be able to handle with any other network transmissions and provide service to the legitimate hosts from which requests are initiated, finally, attacker’s goal of denial service is achieved.

Smurf attack defense

1) Prevention from the source

Attacker resides in a certain network, so all the packets originated from him/her have to go through the router of their network as an exit, generally, the router examines solely the destination IP address but not the source IP address. It is this mechanism of examination that makes a Smurf attack possible. If measures of configuration of ACL access list at the gate of the bounding router that connected to the attacker subnet are taken, permitting only packets originated from 192.168.2.0 network segment, as a result, the forged ICMP packet will be blocked and dropped. Since the blockage the ICMP, the hacker does no harm to other host.

2) Prevention at the bounce site

Because the router at the bounce site will request all the hosts residing in it to answer when it receives the ICMP broadcast packet, thus, mitigation would be to configure the router not to respond broadcast packets. In this case, hosts dwelling in it will not answer the ICMP packets with ICMP echoes. The command in the Cisco router is no IP directed-broadcast.

3) Prevention at the router connected to the victim

Configuring a firewall at the exiting gate connected to the subnet of the victim denies ICMP echoes packets.

3.6 UDP flood attack

A UDP flood attack is also one kind of DOS attack. UDP is a connectionless protocol, which means that no program is needed for the connection before data transmission. A UDP flood attack is launched if an attacker initiates a considerable amount of UDP packets to a victim server. When a victim server receives a UDP packet, it will confirm the awaiting application while it is in search of the destination port. If the server finds out there is no existence of the waiting application at that port, it will generate a port unreachable ICMP packet to the forged IP address, from which the packet came. The target server will crash if it receives a great amount of these kind of UDP packets.

3.7 Ping of Death

Owing to the fact that IP packet length of the IP head is in representation of 16, the maximum length of the IP packet is no longer than 65535 (2^{16}-1) bytes in accordance with RFC791 (Rey 1981). Ping of death exploits this vulnerability. When a victim receives packets of length longer than 65535 bytes from the attacker, this results in the machine crash or restart due to memory buffer overflow while the packet being restructured. Most of the current operating system have fixed this vulnerability with their ability of processing over-sized packets, thus, at present, Ping of Death is an attack of limited threats. What is of great harm is an emerging attack similar to Ping called Ping Storm, which makes the victim busy with handling with the Ping packets, making unavailable to provide service by sending large a quantity of Ping packets.

3.8 Land attack

A Land attack initiates a special poison spoofed SYN packet, with the identical source and destination IP address, to the target. The victim will send a SYN/ACK packet to itself when it receives this kind of request, causing it try to reply itself continuously and establish a connection to itself resulting in a lock up and a considerable degradation in the system performance.

Essentially, all of the types of DOS attack aim to remarkably consume resources like memory, process, disk space, network bandwidth of the target, forcing it to be unable to provide service to legitimate users. What is more, tools used for DOS attack are easy to get in hand, hence, to launch a DOS attack is easy, resulting in DOS attacks pose a great threat to the network security.

3.9 Man-in-the-Middle Attack

A Man-in-the-Middle Attack (MITM in abbreviation) is an indirect intrusion and active attack. By various technical means, a host under hacker's control is virtually placed in between two computers communicating with each other via the network. The computer being controlled is called "man-in-the-middle", which is equivalent to an agent that is able to intercept and modify messages while they are being relayed by the attacker, making the victims believe that they are communicating to each other over a private connection. MITM is a destructive attack of great threats to online bank and online transaction.

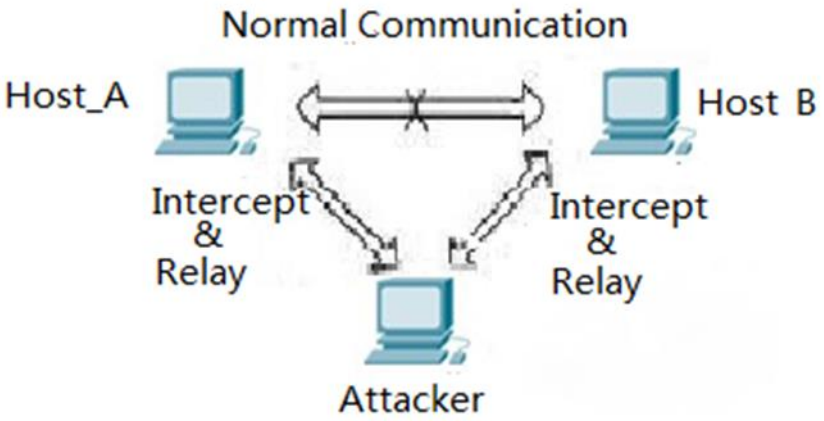

Figure 3.8 Illustration of a Man-in-the-Middle attack

The attacker acts as a "forwarder" when host A and B communicate with each other. As a matter of fact, there exists no a true communication between them, all the messages that they exchange are relayed by the attacker who plays a role as an intermediary host without both host A and B' awareness of it but they mistakenly believe that they are talking directly to each other. Therefore, the attacker host acts like a transponder within his/her ability not only to eavesdrop

host A and B's communication but also, before forwarding, to falsify the messages and inject malicious information in it.

Theft of information, rather than the attacker forwarding the message, but backup the data while being transferred between host A and B is performed to attain user's sensitive information such as account and password.

Main methods of MITM attack

1 Key Manipulation

By interception and modification of the public keys exchanged by the client and server, the MITH attacker alters the communication flow, afterwards, all the communication will be forwarded by the hacker host, which is performed without the client and server's knowledge, Before relay, the MITM attack is able to both eavesdrop and modify the communication being transferred between the victims for further attack.

2 Injection

To add packets to the established connections, an attacker is able to modify the sequence number and keep the connection synchronized while injecting malicious packets without the changing of the communication flow for instance, to inject commands to the server and to emulate fake replies to the clients.

3 Downgrade Attack

To reduce the difficulty of attack, the attacker forces, by the means of modification of the communication data, the client and server to employ less secure features, function or protocols which are provided for the backward-compatibility with the older versions applied by the clients and server. Sometimes, clients support accesses to the server with different features or the same feature but with different versions, as a result, by consulting, clients and server decide what feature and feature of which version is supposed to applied.

Actually, a MITM attack is an combination of interception, eavesdropping, selective modification of data to achieve the attacker's own goal. ARP spoofing and DNS spoofing are two major types of MITM attack (Akshaya & Katebarry 2008)

.

3.10 ARP Spoofing

ARP protocol

The ARP protocol is an abbreviation for "Address Resolution Protocol". It is one of the protocols at the bottom layer of the TCP/IP protocol and functions as

translation from IP address to the corresponding MAC address for the reason that gateway needs to know the target host physical address to fill the physical frame of the destination address when two hosts in the local area network communicate with each other or the host in the local area network forwards IP data to the gateway. “Address resolution” means the act of translating from the target IP address to MAC address. In other words, ARP plays a role in ensuring the successful communication by inquiry of the target host MAC address based on its IP address.

In a local area network, it is a must to know the target host IP address for communication with one another, however, what is identified by the physical device, like the network interface card which finally takes the responsibility of data transmission is not IP but MAC address. As a result, in a local area network, communication between hosts necessitates the knowledge of the one counterpart’s MAC address. It is the ARP cache table that assists in accurately acquiring one’s opposite side’s MAC address of the network interface card. An ARP cache table, for every host in an local area network, serves as a container keeping all the known mapping of the IP address and MAC address of every host in that local area network. A host will inquire the mapping in the ARP cache table before it sends out data to another host. Generally, the mapping will be valid for no more than twenty minutes (Blank 2002).

A local area network will be simulated for the explanation of the how the ARP works.

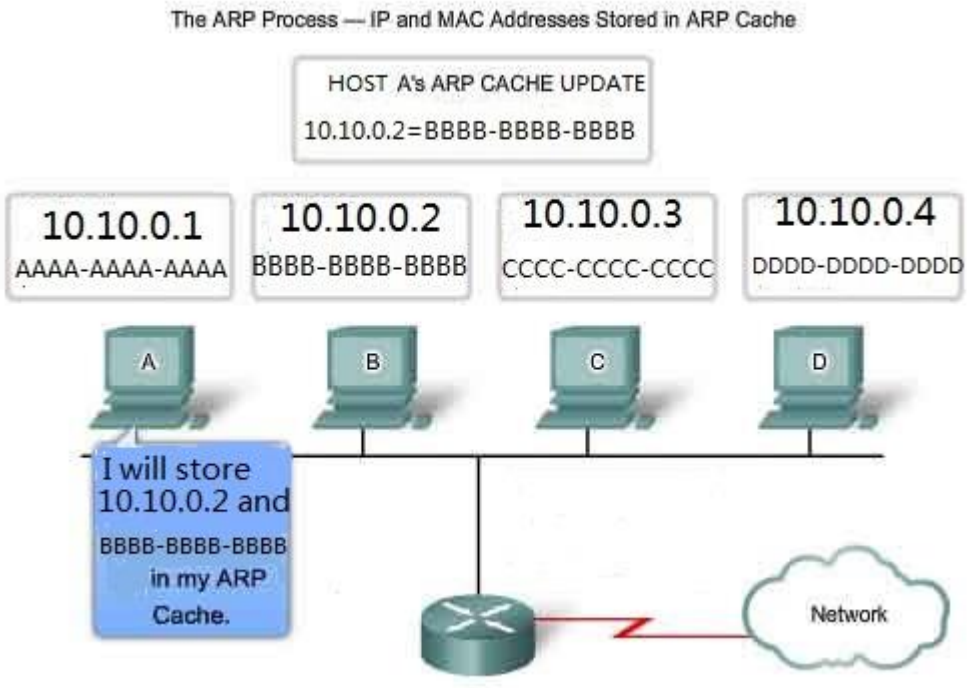

Figure 3.9 Illustration of how ARP protocol works

(www.google.com.hk)

Initially, suppose the ARP cache table of host A is empty or stores no information about host B and Host A wants to communicate with host B. However, the problem arises when host A tries to transmit data to host B because the MAC address of host B is not known to host A. So A checks the ARP cache table of itself to determine whether the presence of the host's MAC address with IP address 10.10.0.2, if yes, BBBB-BBBB-BBBB will be encapsulated at the packet and sent out afterwards; if no, host A will issue an ARP broadcast packet with a message that my IP is 10.0.0.1, MAC is AAAA-AAAA-AAAA and what is the host's MAC address with IP 10.10.0.2. Including host C and D, all the hosts receive that ARP broadcast packet, which will be dropped by host C and D as soon as they know it is not their IP addresses that is wanted. Subsequently, host B will reply, instead in the form of broadcast, but solely to host A that I am the one with IP 10.10.0.2 and my MAC address is BBBB-BBBB-BBBB, which is now known and attached to the packet by host A before the transmission to destination. Simultaneously, the ARP cache table will update by adding 10.10.0.2-BBBB.BBBB.BBBB in it. Therefore, host A does not need to send an ARP broadcast inquiry the next time when it communicates with host B. This is the whole process of how the ARP protocol sends packets.

ARP Attack Principle

After the introduction of how the ARP protocol works, it can be concluded that the communication mechanism that all the hosts in the local area network are reliable. In other words, that means all ARP packets initiated from whatever the hosts are absolutely correct, which is a jeopardous assumption and makes this mechanism as fatal flaw of the protocol for the reason that not every host abides the rule as it is supposed to. Take Figure 3.9 for example, when host A inquires to the whole local area network for what the host's MAC address with IP 10.10.0.2 is, host B reply with its correct MAC address, host C, who is not what host A that looking for, replies that its IP address is 10.10.0.2 and its MAC address is CCCC-CCCC-CCCC, so what host C does is that it lies to host A and imitates host B. Before host C replies, the ARP cache table have already kept the correct mapping of host B 10.10.0.2-BBBB.BBBB.BBBB, however, the ARP cache table updates and the correct mapping 10.10.0.2-BBBB.BBBB.BBBB is overwritten with the wrong mapping 10.10.0.3-CCCC.CCCC.CCCC as a result of host C's incessant replies and host A's unawareness of the forged packets generated from host C. This process is called ARP attack with technical name "ARP Cache Poisoning". Therefore, from now on, when host A sends data to host B(10.10.0.2), all the sent data will be forwarded to MAC address CCCC-CCCC-CCCC, which is host C, consequently, host C hijacks the data initiated from host A to B. This is how ARP spoofing works(Ye 2008).

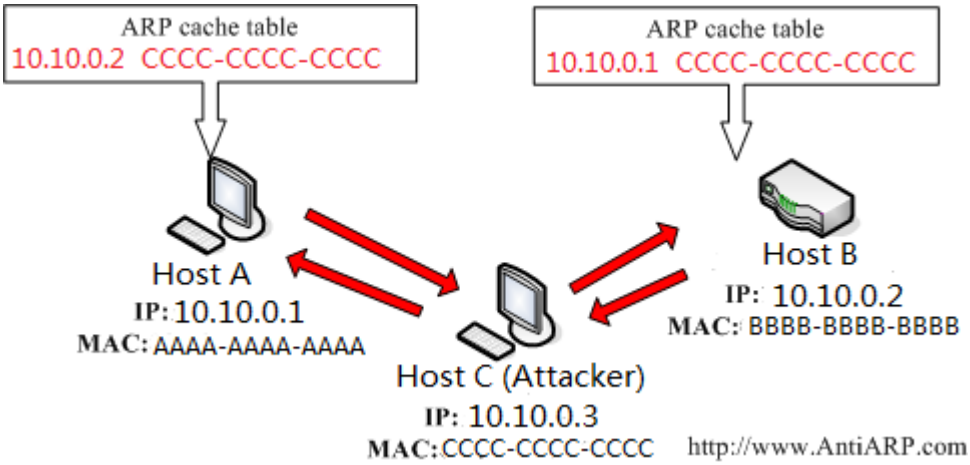

Figure 3.10 Illustration of ARP spoofing process

(www.google.com.hk)

ARP spoofing process:

1. Host C (attacker) takes initiative in replying to host A's ARP packet, informing A that IP 10.10.0.2's MAC address changed to CCCC-CCCC-CCCC (original MAC address in the ARP table is BBBB-BBBB-BBBB).
2. Host C again takes initiative in replying to host B's ARP packet, notifying B that IP 10.10.0.1's MAC address changed to CCCC-CCCC-CCCC (original MAC address in the ARP table is AAAA-AAAA-AAAA).
3. When host A communicates with host B, actually data intended for B is forwarded to host C and the same is true while host B transmits data to host A. As a result, host C becomes the "man-in-the-middle".

Defense Against ARP Spoofing

1. Static ARP Table

The adoption of ARP static table can be used to guard against ARP spoofing by configuration of the static address mapping on the target ARP cache. Rather than updating automatically, the mapping is configured manually, as a result, configuration of the ARP cache is performed every single time when there is a change of the host's IP, which means a considerable amount of workload will be needed for the maintenance for the updates.

2. Division of Secure Region

Generally speaking, an ARP broadcast packet is not able to travel across the subnet and network segment, which, in other words, filter the ARP broadcast. A VLAN (Virtual Local Area Network) is a logical broadcast domain. Isolation of

the broadcast in the local area network can be realized by VLAN, creating multiple subnets. When detecting an ARP attack by a hacker, the administrator tracks and locates which switch port that host connects to and, isolates that host from other hosts by assigning a specific VLAN to it, which reduces the impact to other hosts (Vivek & Sukumar, 2013).

3.11 DNS Spoofing

DNS is abbreviated as Domain Name Server. In the Internet, a way to distinguish from host to host is by using IP address, which is represented in digits without any special meaning, making it difficult to be memorized by the human brain especially when these numbers are lengthy and irregular. As a result, a host is given a specific name, with some kind of meaning, which are prone to be memorized and is called “Domain Name”. For example, when people want to visit Google, they tend to type http://www.google.com in the web browser rather than the IP of the server 8.8.8.8 which is also feasible, therefore, http://www.google.com is the domain name of Google which is similar to how people greet when they meet by their names instead of their ID number. Owing to the fact that what makes host distinguishable is their IP, the browser has to inquire from the server where the mappings of domain name and IP address are stored, after users type in the domain names. The server being inquired is what we called “Domain Name Server”.

How DNS works

DNS is composed of two section: server and client. The port number which requests exits and entries to the server is 53. The first act a local DNS server will take, when a client initiates a resolution request to the server, sends an enquiry to the database about whether the required content is stored in the database. If yes, the local DNS server will reply with the corresponding the mappings, if not, it will enquire the DNS server of upper level and recursively acts in this way until the relevant result is found or return an information that fails to find the enquiry from the client. If the local DNS succeeds in finding the required information, before replying to the requesting client, it will store the found mapping in its cache, in this way, future repetitive requests of the same enquiry from other hosts, rather than again search from server to server, but can directly be extracted from the cache of the server for that mapping and reply to the client.

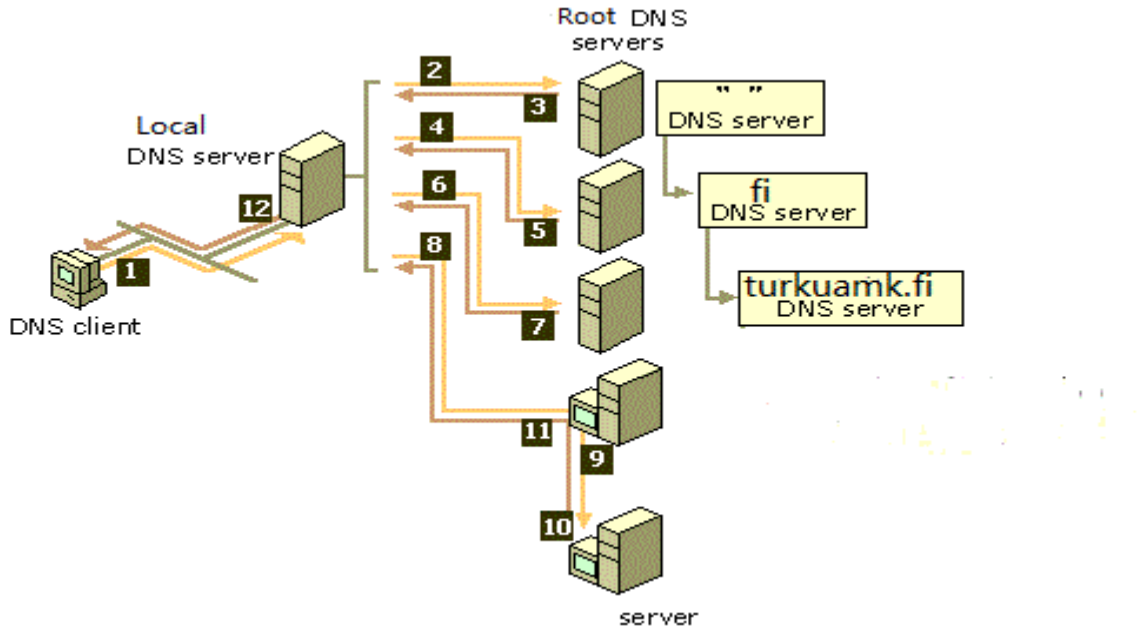

Figure 3.11 Illustration of how DNS protocol works(With modifications)

(www.google.com.hk)

Assume the client's IP is 10.0.0.1 and the Turku AMK DNS server is 192.168.0.1, through which client visits the website of Turku AMK. After typing the domain name of the school www.//turkuamk.fi in the browser, the corresponding IP address can be obtained through the DNS server.

Step 1-2: Sent from a random port of the client 10.0.0.1, though port 53 , the request was received by the local DNS server 192.168.0.1 and translated. Then, the local DNS server searches from its cache for the IP of the www.//turkuamk.fi; if the relevant mapping exists, then it will send it back to the client and if not, it will look it up in the root server.

Step 3-10: The Root DNS server receives the request and returns the address of the fi domain server to the local DNS server. It then issues a request to the fi domain server, which returns the address of the turkuamk.fi domain, again generating request and the address of www.//turkuamk.fi is obtained.

Step 10-12: After DNS responding packet, the local DNS server forwards to the client after the possession of the translated address. Later, the client will examine the ID and the port number of the packet, after receiving from the DNS server, to check if they are identical as they are sent out at first. If yes, the DNS response packet is accepted as valid and then connection between the client and the webpage is established. If not, a repetitive response packet from the same domain name is considered invalid and dropped (Krawetz 2006).

DNS ID Spoofing attack principle

DNS ID spoofing attack is launched depending on the condition of ID surveillance and port number and ARP spoofing is also involved. First, the intention of the attacker is to modify the content of the ARP cache. To achieve this, he/she will repeatedly generate forged ARP request messages to the target, causing the data flows towards the attacking host before the destination. Afterwards, the hacker get the ID and port number in hand by sniffer software use on the surveillance of DNS request packet. At the possession of the ID and port number, a forged DNS response packet along with the fake ID will be sent from the attacker. After the victim completes the transmission it will verify the ID and port number, supposing the ID and port number are real and correct from the DNS response packet and consequently accept the packet. On the contrary, the real original address that the victim plans to visit at first is already modified and replaced by the fake one that directs the user to a malicious website where it is not expected to visit and poses a threat to the information of the victim. Up until this moment, all the future DNS response packet from the DNS server will be discarded by the user as a result of it being left behind. Therefore, the address the victim will visit is the one that attacker set as a trap with the purpose of interception of information and so on (Krawetz 2006).

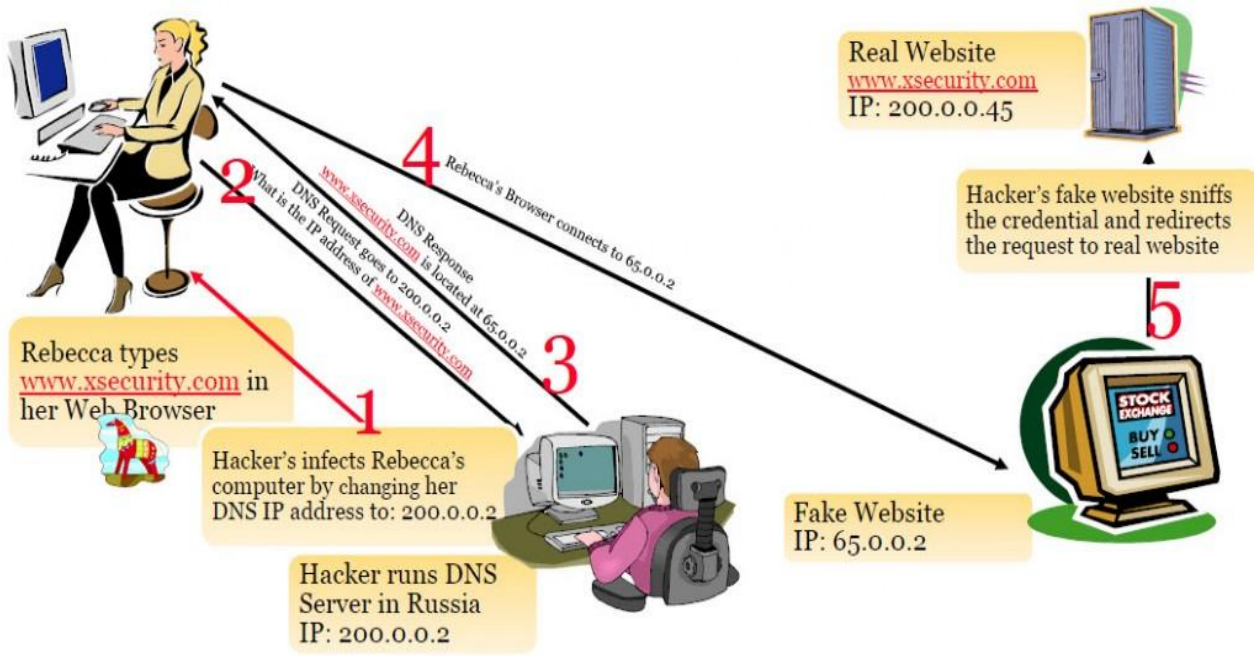

Figure 3.12 Example of a DNS spoofing attack

(www.google.com.hk)

A DNS spoofing example

Suppose the fake IP is 65.0.0.2 , Rebecca types www.xsecurity.com and sends the recursive resolution request to the local DNS server. The process goes as below:

1-2. The victim is being monitored and a request is captured by the attacker. After that, the DNS request will be directed to the one that designed by the hacker.

3. As a fake packet message, the DNS response notifies the victim that the corresponding IP address of www.xsecurity.com is 65.0.0.5.

4. The launched attack is successful, making the victim to direct to the fake IP address.

Defense against DNS Spoofing

1. Visit by IP address

It is advisable to prevent the use of DNS when visiting some specific websites, which require of high level of security, by direct use of IP address without DNS resolution. In this way, there will be no way for the attacker to launch DNS attacks. The reason for this suggestion is due to the fact that DNS attack aims at the theft of the user's private information which does not occur in websites of that kind. What is more, this mitigation has little negative influence on other services and network environment, as a result, a visit by IP address is an easy measure of high effectiveness.

2. Binding IP address with MAC address

As mentioned in Section 3.12 DNS spoofing exploits the IP address which in disguise or alters that of the DNS server, owing to the fact that the feature of network interface card MAC address is globally unique binding it to its corresponding IP address and storing the mapping to the client can prevent DNS spoofing attacks. Clients will, from then on, verify the DNS response packet issued from the DNS server. By comparing the mapping in its own storage with the one receives from the DNS response packet, it can be concluded whether the response packet is DNS spoofing attack.

4. Network Security Defense Technology

Technically speaking, network security is mainly composed of secure components such as firewall, intrusion detection, antivirus and so on, any of which works independently without assistance from other components is incapable of securing the network information. In other words, there exists no a defense technology which is good enough to assure the security of the network information service. As a result, for an effective mitigation of network threats, a combination of diverse technologies is applied intending to extend the time it takes for the attacker for intrusion and increase the cost and the necessary resources, with the goal to protect the network at large extent. Currently, the common network security defense technologies are firewalls, Intrusion Detection System, access control and so on.

4.1 Firewall Technology

Owing to the openness of the network and increasing enhancement in the attacking , the issue of security is becoming more complicated and network defense is not the same as it used to be. The emphasis of the network management was on centralization and concentration, for instance, application of encryption, access control, authentication and security audit for defense. In the circumstance the Internet is placed nowadays, the urgent problem we are encountering is how to secure our communications through the Internet so that daily normal communication is guaranteed, what is more, internal networks are not subject to attack from external networks. It is known that, while in the process of communication, it is inevitable that an attacker will gain illegal access to the internal network for theft of information or undermining. This accounts for the reason why it is important that internal network should be free from external network attack during communications. Under the circumstance of the security problem the firewall, or what we generally call the earliest products of network security equipment, came into existence.

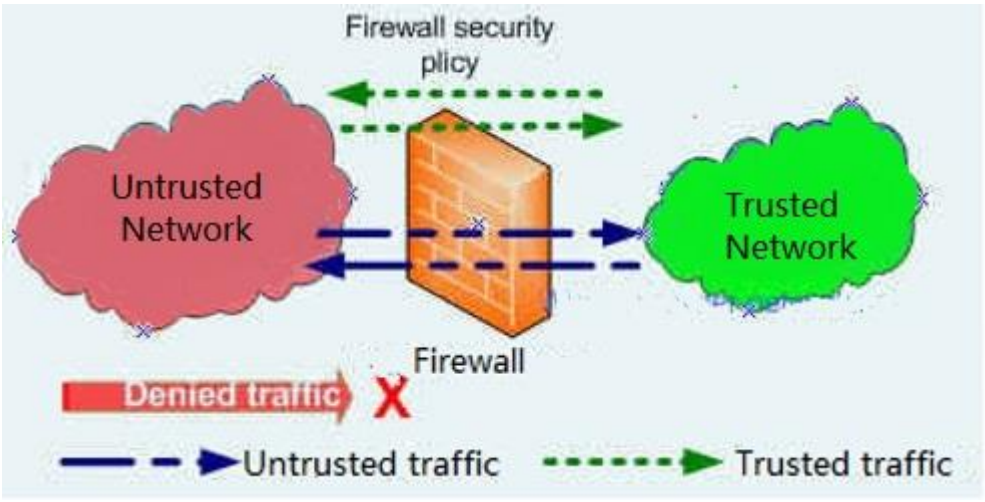

Figure 4.1 Example of a firewall

(www.google.com.hk)

As can been seen on the right-hand-side of the figure, there is the Intranet which is composed of trusted hosts. Untrusted hosts on the left-hand-side build up the external network which is what is called Internet and some trusted hosts might be also inside it. Through firewall and routers, hosts inside the intranet are able to receive traffic from the Internet. As a conclusion, basically a firewall insolates untrusted networks from trusted networks.

4.2 What is Firewall?

By definition, a firewall is a special network interconnection software designed for the promotion of the access control between networks. What is more, it is a remarkably effective network security model, which functions as the

construction of relatively security subnet out of the insecure networks environment, in other words, to isolate subnets from the Internet for security reasons. As illustrated in Figure 3.13, a connection is established in between the untrusted network and the trusted network, as a result, all the inbound and outbound traffic between the intranet and extranet has to be examined while it travels through the firewall. Under the operator's monitoring and control, consequently, only the traffic in accordance to the pre-defined inflow and outflow access control policy is permitted.

The data link layer, the application layer and the network layer are the three layers of the OSI model at which a firewall is implemented. The essential characteristic of the firewall is operated for isolating an intranet from an extranet and access control implemented on in-out information. Isolation can be achieved physically and logically. Logical isolation means that a firewall not only serves secluding an intranet from extranet, but also further segregating the secure network, that is to say those sub-networks requiring for different security requirement can be sub-divided by firewall based on what they need. As a result, a firewall do not have to be installed where the extranet is connected, instead, it can be installed at different domains of the same intranet. For instance, for the same corporation who has many different departments such as research department, financial department, which are not equally the same in the security strategy. As a conclusion, a firewall is used as logical isolation device.

From the perspective of defense system, a firewall is a passive defense device which means, instead of automatically creating a new policy for the defense of changing attacks, the protection is achieved by a pre-defined fixed strategy when it come into force. Generally, the scheme of a firewall is drawn by the administrator based on a corporation's or department's security strategy needs.

4.3 Firewall Functions

1. Network Security Barrier

Protection of the intranet is performed by blocking of the illegal attack and information flow from the extranet.

2. Filtration of insecure services.

A firewall lays its control on bi-directional in-out data flow between the intranet and extranet.

3. Prevention of specific network attacks

A firewall is a passive defense which means that it is incapable of mitigating dynamics attacks. A firewall works with other network devices to guard against specific attacks. For instance, a firewall with Intrusion Detection System(IDS), which is used as a sensor placed where it is needed for network information flow inspection, intends to make comparison to decide if the inspected flow meet the characteristics of certain of attack. The pre-defined static security policy configured on the firewall is not able to add a new item which is not

deployed when it finds out a new attack is ongoing. After a firewall's interconnection with IDS, IDS will offer to contact with firewall when the attacking flow is detected, making the new strategy to be automatically added to the firewall security policy list thus preventing that ongoing attack.

4. Deployment of NAT

NAT is an abbreviation for Network Address Translation for the use of concealing of the internal topology and relief the IP address shortage, allowing multiple hosts to share one single legal IP address connected to network. For instance, a school local area network whose hosts IPV4 addresses are composed of internal addresses of the LAN. Thus ,these addresses are not routable and illegal. Deployment of NAT on the firewall is a solution for multiple hosts residing in a small LAN, sharing the same IP address for connection to the Internet. As a result, a firewall is favorable place for the deployment of NAT.

5. As a site for monitoring and early-warning for LAN security

A firewall, aims to establish one and only one connection, at which all the traffic going through firewall has to undergo examination. This inspecting mechanism enables the firewall to perform security statistics collection and analysis if monitoring and auditing is enabled on it for the convenience of the administrators' examining the data when needed. In this way, security and system maintenance are enhanced.

4.4 Firewall Classification

1. Personal Firewall

What is in use by ordinary users nowadays is classified as "Personal Firewall". Software, such as Norton and McAfee belongs to this type, which is operational on the operating system providing a simple firewall service for personal computers. Take the Norton personal firewall for example, it is mainly concerned with the communication of the installed host with other hosts and the security issues with the Internet, rather than security issues between networks which it is not the same job as it is performing as the perimeter firewall discussed above.

2. Software Firewall

At the same time, the personal firewall mentioned above also belongs to software firewall, however, the applications of personal firewall are limited and not as many as software firewall. What is more, the personal firewall is poor in security and concurrent connection processing ability resulting from the possibility that its chip processing is software-based instead of hardware-based. As a network firewall, software firewall is better in control ability and performance than a personal firewall. Personal firewall's sub-classification accounts for its better applications and functions comparing to other software

firewall which is network-based software firewall supporting operating system Unix, Linux in addition to Windows. Some famous software firewalls are the Zone Alarm and Check Point firewalls.

3. Ordinary Hardware Firewall

Ordinary hardware firewall is neither equivalent to genuine hardware firewall which is composed of special chip, not to pure software firewall because there is a huge difference between them. An ordinary hardware firewall is an embedded host, whose components can be customized. Ordinary hardware firewalls are generally developed by small firewall companies whose target customers are small and medium-sized enterprises. An ordinary hardware firewall features in full-function with average performance. Full-function refers to the security audit feature, NAT and so on, which are composed of the firewall function, while performance means parameter index such as the throughput capability, concurrent processing ability etc. Compared with the genuine hardware firewall, the ordinary hardware firewall has far less superior performance.

4. Hardware Firewall

A hardware firewall is made up by dedicated chips which are designed for processing of the crucial strategy of the firewall. Therefore, along with the increase in the number of concurrent connection and throughput ability, the performance of a hardware firewall also benefits from these features and is boosted remarkably.

5. Distributed Firewall

The types of firewall discussed above are perimeter firewalls. As the name indicated, it might be imagined that the place where they are usually located is the network boundary. The spot usually either is the border connecting intranet and extranet, or between different security domains. The drawback of the perimeter firewall is its failure to provide effective protection to the intranets. As the evolution of the network and the attacks are developing, a new firewall architecture came into existence called “Distributed Firewall”. In recent years, some network device developers and companies have been devoted in the this technology. However, questions such as what the trend will be for this technology in the future or when it will be put into use are remain uncertain. These uncertainties result from the fact that it usually takes a considerably long time from technology research to technology maturity then finally to production. Theoretically speaking, a distributed firewall is a superior defense architecture, however, when it comes to practical point of views, it remains uncertain.

4.5 Firewall Limitations

1. The network security we generally refer to is achieved at the sacrifice of openness and flexibility of network service. Suppose an enterprise network is fairly secure, it might be noticed that some daily communications are restricted, for instance, failed use of web surfing or instant messenger while working,

inaccessibility of external websites for the reason of possibility that addresses from these websites are within the range of untrusted networks. As a result, an increase in network security might concur with a decrease in openness and flexibility of network. This is one of the reasons accounting for the firewall limitation.

2. The use of firewall leads to the weakening functions of network, which actually relates to the feature of openness. For instance, a firewall is mainly used for logical isolation protecting the intranets simultaneously, the information being exchanged with the extranet might be interfered, in other words, a firewall, as an intermediary agent through which traffic has to go, causes the intranet to be unable to directly communicate with extranet. To conclude, to some extent, a firewall impairs a network functions.

On a firewall, it is possible to append software, which is proxy service a guarantee of better network security. If an IPP(Internet Printing Protocol) proxy is installed on firewall, intranet users who intend to use the IPP service, have to go through the authenticated proxy server which will first authenticate users to decide if they are in accordance with the security strategy. Afterwards, the IPP request will be forwarded to the real IPP server only in the case that it is up to the suggested requirements. In other words, the proxy plays a role in blocking the users' connection with the real IPP server from the extranet. Therefore, there will be a drop in management overhead, transmission rate etc.

3. A firewall is not able to solve attacks and security issues originated from the internal network. For instance, some pre-defined strategy is effective for internal networks, but not the intranet. This is because the intranet generally is a trusted network which is difficult to guard against.

4. Only illegal access and attacks which go through but not go around the firewall are defensible by firewall. If a hacker succeed in bypassing, the firewall is useless as if it is not existent. As a conclusion, a firewall is not expected to be an absolute guarantee of network security.

4.6 Firewall Architecture

Organizations and systems should decide what a firewall is most suitable for them own selves based on risk assessment and security requirements. As a result, knowledge of firewall architecture is beneficial in the selection of firewall according to the network and security demands.

What is Firewall Architecture?

A firewall system implements the selected structure. It is important to know the firewall architecture for the reason that it determines the functions, performance and range of applications. There are four firewall architectures, packet filtering

firewall, dual-homed host firewall, screened host firewall and screened subnet firewall.

4.7 Packet filtering firewall

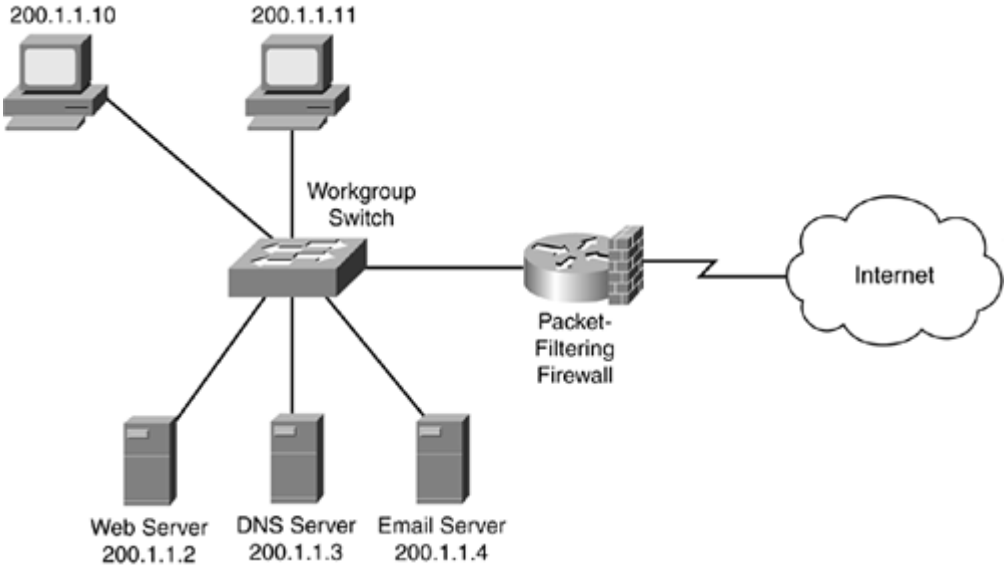

Figure 4.2 Example of a Packet filtering firewall

(www.google.com.hk)

Packet filtering firewall can be achieved either by a dedicated router or a computer. In Figure 4.2 the router functions as a firewall. This is a simple topology of a packet filtering firewall, which allows the hosts from the protected network(trusted network) to directly communicate with the hosts from the Internet. Thus, the vulnerability lies in the router on the hosts inside the protected network and the accessible services, resulting in a risk that the security goes down as the number of the internal hosts as well as the types of the services being accessed grow. Note that a packet filtering firewall is the sole passage between the internet and extranet requiring the exchange messages to be examined if in accordance with the security policy when going through. Filtration is achieved at the installation of the IP layer packet filtering software on the packet filtering firewall.

A packet filtering firewall is simple in its structure and topology. It is easy to install and implement with a single computer or router. However, the limitation is low security manifested in its failure of supporting user authentication and limited logging capability. As it might be known that it takes a little effort to forge IP addresses, there is no way for the firewall to differentiate hosts who are sharing the same IP address if no user authentication is available. For instance, suppose an IP address spoofing attack is launched and host A is an legal user. If host B alters its own IP address to the same as host A, in the packet filter firewall environment this means that no user authentication and hosts identification based solely on IP address packet originated form the illegal user

host B will be permitted. A danger might ensue and this accounts for its low security (Preetham 2002).

4.8 Dual-Homed Host Firewall

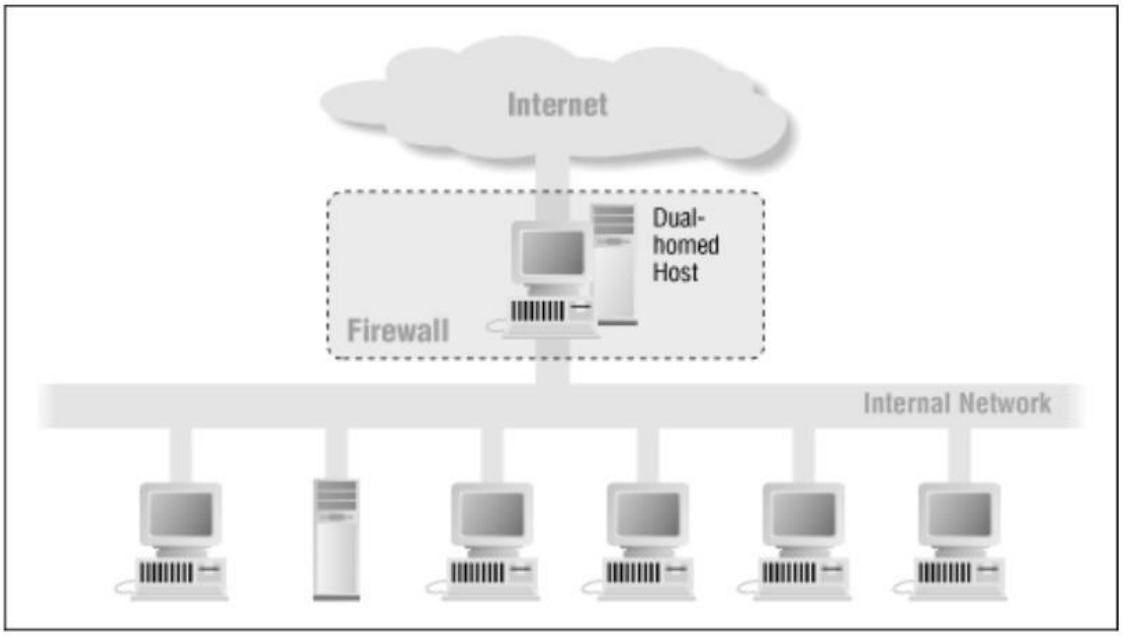

Figure 4.3 Example of a Dual-homed host firewall

(http://docstore.mik.ua/orelly/networking/firewall/ch04_02.htm)

In Figure 4.3, there is an essential difference with the packet filter firewall that is that packet filter rule is not applied in this example. If internal hosts visit websites from the extranet, they have to be authenticated beforehand by the proxy server which is the dual-homed host firewall. As its name indicated, a Dual-homed host firewall is a bastion host which possesses double network interface cards and its location is in between the protected network and Internet. Rather than by the application of packet filter rule, the dual-homed host firewall functions as a prevention of IP layer communication by implementing the traffic between the intranet and extranet through the application layer.

For the convenience of the user and management, the way to implement dual-homed host firewall function is by proxy service. It is important to note that IP layer communication is completed blocked in the dual-homed host firewall environment, which, to a certain extent, is an improvement in security. It is also to be noticed that firewall software is operational on dual-homed host firewall. The installed firewall software serves to provide services. For instance, an internal host who wishes to use the IPP service needs to be authenticated by the proxy server to determine whether the host meets the pre-defined strategy and it is a legitimate user, thus, the installation of firewall software on a dual-homed host firewall is beneficial to the improvement of the system security.

A dual-homed host firewall is able to be used for authentication and logging, which is advantageous for security audit. By recording of traffic flow through the proxy server, the security audit might be able to trace the source of hacker in case of an attack and offer useful information for the analysis of the network security situation. The inflexibility of the dual-homed firewall could be a disadvantage to some websites for the reason that all services requested from the intranet to the Internet are blocked (Preetham 2002).

4.9 Screened Host Firewall

A Screened Host firewall offers more flexibility to implement and more secure compared with the two firewalls discussed above.

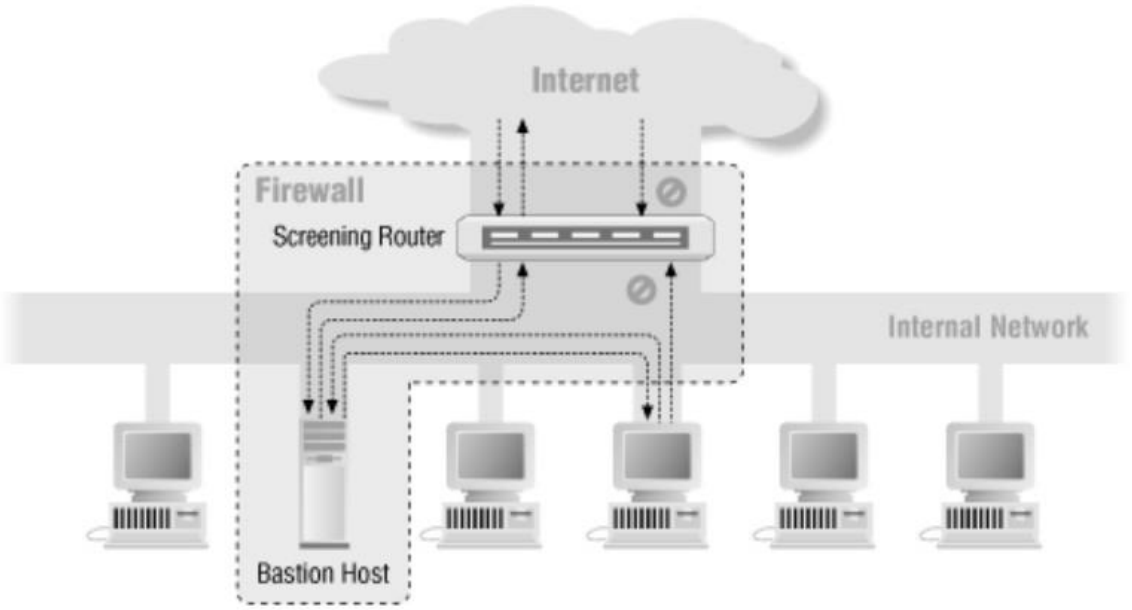

Figure 4.4 Example of a Screened Host firewall

(http://docstore.mik.ua/orelly/networking/firewall/ch04_02.htm)

As can be viewed from the Figure 4.4, the components enclosed in the dotted line are Screened Host firewall, which is made up by a packet filtering firewall and a bastion host. Generally, in a Screened Host firewall topology, a packet filtering firewall plays a role as a connector with the Internet while, at the same time, a bastion host on which gateway software is operational is installed in the internal network. Besides, filtering rules are set up on the router with the intention of making the bastion host as the one and only one, located in the intranet, that is able to directly communicates with the extranet. In other words, no internal hosts, with the exception of bastion host are able to exchange traffic with Internet. This is the idea of application of a Screened Host firewall.

Two measures are applied packet filtering at network layer and proxy at the application layer installed on the bastion host, therefore, Screened Host architecture is a firewall of high level security. The proxy forces traffic from the extranet to go through the bastion host. The same is true for the traffic originating from all other the internal hosts. Note that the proper configuration of the packet filtering router is the key to the success of the screened host firewall, which responds to the appropriate filtering policies being enforced. One major disadvantage of the screened host architecture is that if the router is compromised, the possibility of bypassing of the bastion host might ensue leaving the entire intranet to be available to an attacker. To be conclude, in the Screened Host firewall architecture, the router is supposed to be in absolute protection (Preetham 2002).

4.10 Screened Subnet

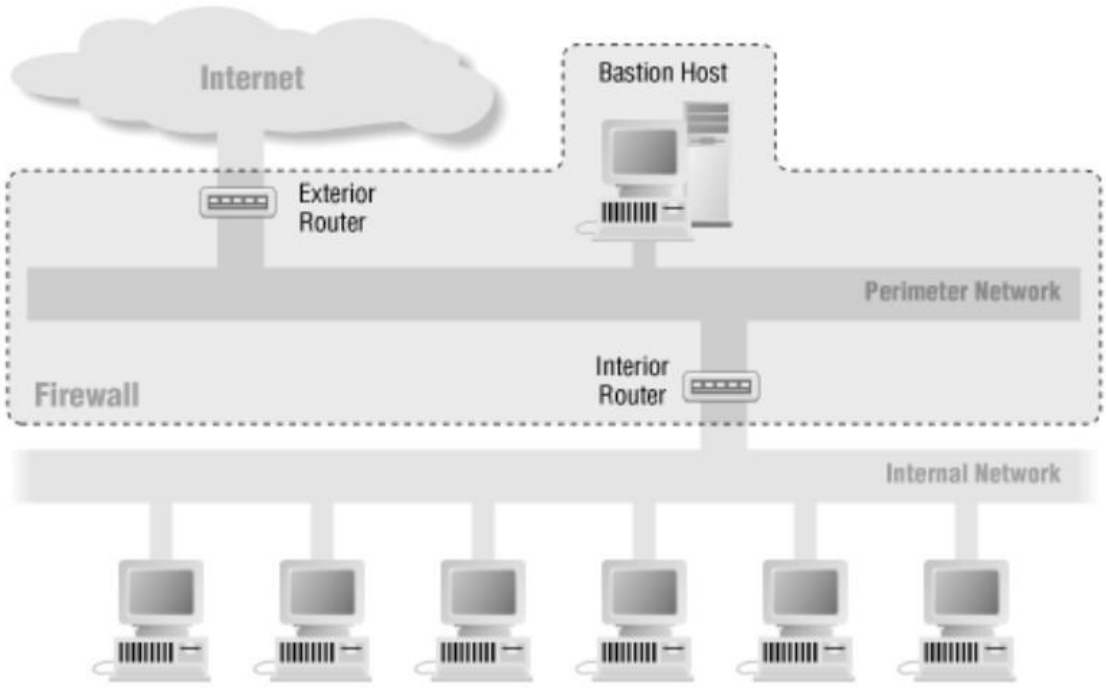

Figure 4.5 Example of a Screened subnet firewall

(www.image.baidu.com)

Among all the four firewalls discussed in this chapters, the screened subnet is the most secure architecture. It mainly features in the exclusively creation of an isolated subnet called Demilitarized Zone (DMZ in abbreviation) which consists of bastion host and servers. Therefore, DMZ serves as a service provider for the reason that servers residing inside. Figure 4.5 presents a common topology of a Screened subnet. As can be viewed from that figure two packet filtering routers, placed in the both sides of the network, are accessible from either the

intranet and extranet, which makes up a screened subnet intended to forbid communications to be traversed. The advantage of this structure is that, attacks generated from external to internal, attacks can be prevented at the external router. Before arriving at the intranet, external packets have to be examined by the external router for access management and then go through the screened subnet. After incoming packets are permitted by the external router and go through the bastion host, the internal router acts as a gate to allow to go further into the intranet based on the security policy enforced on it (Preetham 2002).

Note that bastion host tends to be the vulnerable target for intensive attacks. Apart from providing services, DMZ also serves as an isolator. Assuming the bastion host is taken down, the entire network becomes the easy prey of the attackers in the Dual-domed Host firewall architecture, however, in the Screened subnet architecture, the loss of the bastion host will not result in an attacker's ability of listening to the session with DMZ interference. This double protection makes the bastion host not the single point of failure.

5. Intrusion Detection System

As Internet features in being open and available to anyone, it results in a diversity of security issues in computer-based network system. Furthermore, solely relying on passive defense, such as firewalls, is not sufficient and advantageous to network and system operation. This accounts for the fact that although a variety of security devices and tools, security policies are applied to assure the daily system operation, there exists a number of risks which are hidden and hard to be detected in the network security.

Every security measure is limited within its range and environment to effectively perform its job. Hidden dangers are:

1. Hidden dangers in firewall

Being a network defense technology of high effectiveness, a firewall is able to keep the internal network hidden and serves as a gateway restricting insecure external traffic from entering the internal network. However, a firewall is incapable of preventing attacks originated from the intranet along with attacks bypassing it.

2. Hidden dangers in access control

Awareness of the requested host holds the key to the success of the access control. As a result, intruders in disguise of the requested hosts take little effort in deceiving the access control mechanism. Besides, improper configuration of the access control will result in serious risks.

3. Hidden dangers in system backdoor

System backdoors are usually the factor of not sufficient attention to traditional network defense technologies. For example, system backdoors traffic which, in the firewall's point of view, is ordinary flow, will bypass firewall if it is not taken into consideration.

Various factors render the network fairly problematic, thus, close attention should be aroused to those factors. To enhance security, the idea of, instead of solely passive, a more active defense technology was brought forward as a measure of higher effectiveness and power against the hidden dangers discussed above. Intrusion Detection System is one of these technologies.

5.1 What is an Intrusion Detection System?

An Intrusion Detection System(abbreviated as IDS onwards) is a technology which is dedicated to discover the existence of violation against the security policy, or, the sign of being attacked in the network or system, by the means of information collection at the key points at which dwelling computer network or system for analysis. IDS is a combination of software and hardware, originated from audit technology which is a process of system event logging intends to perform recording and examining in chronological order.

5.2 IDS structure

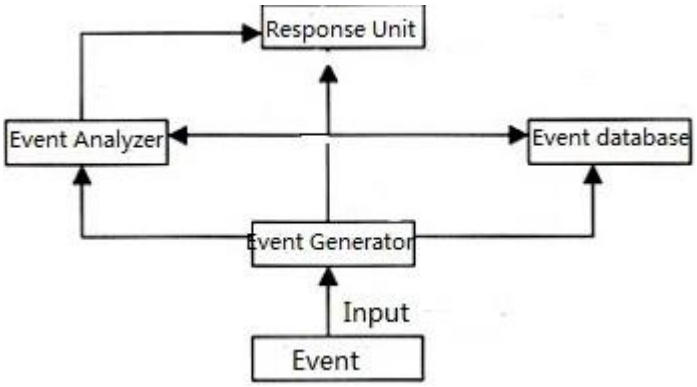

Figure 4.5 Example of a IDS Structure

(www.image.baidu.com)

Generally, IDS is composed of an event generator, an event analyzer, an event database and a response unit.

1. Event generator

It mainly functions as a collector of raw data used for transforming events into output. Afterwards, event generator will notify the output of the event to other parts of the system. The target information includes the status and behaviors of the users as well as system and network data. The implementation is carried out by multiple key points, located in the network system, installation of sensors for data collection from different network segments and hosts. Note that the success and effectiveness of the IDS, to a large extent, rely on how accurate is the collected information. As a result, it is necessary to assure of the integration

of the software intended for the detection of network system, otherwise, inaccurate information will mislead the administrators to a wrong conclusion.

2. Event analyzer

An event analyzer serves as a receiver of event information for analysis to determine whether an event constitutes intrusion or abnormal behavior. That is to say, the judgment, is only made after the analysis, and finally it is turned into alarm information.

Ways how to implement event analyzing (Dapeng 2006)

a. Mode matching

The prerequisite is the creation of the network intrusion and system misuse mode database in which known intrusions, such as DOS or other attacks, are recorded. By comparing the newly collected information with database, any violation of the security policy will be detected if there is any. In conclusion that is performed by matching.

b. Statistical Analysis

Statistical analysis, fundamentally different from mode matching, is an initial establishment of a descriptive statistics for the system objects, such as administrator, user, file typist, important directory, security devices and so on, by statistical technique. What is include in the statistical figure is a measurement attribute when is under ordinary use. Take a certain system object user for example, the frequent act a system network administrator performs when he/she logins in file operations such as directory creation, file deletion and modification and so on for maintenance, or, examination on logging for analysis. For a logged typist, file edition would be a proper regular task, therefore, it would be an alarm if he/she conducts acts related to system file like name and attribute modifications. Once detected by IDS that a logged typist acts like a network administrator, suspicion of typist's privilege escalation or even an intrusion should be aroused. This accounts for the need for establishing descriptive statistics, which make measurements (such as number of visits and operation failures and so on) under normal use.

3. Event Database

An event database functions as a storage of raw and processed data received from the event generator or event analyzer. These data are afterwards stored for a considerable long time for future use when required.

4. Response Unit

The reason that IDS is considered to be an active defense is the introduction of the response unit. Alarm generated as a result from the event analyzer will be provided as a clue how to react, for example disconnection to cut off the attacking flow or trigger an alarm as a notification to the administrator.

5.3 IDS Classification

There are two categories of the IDS in terms of the classification Analysis-based, Data source-based

1. Analysis method-based IDS

The two most important parameters which determine the performance of the IDS are false positive and false negative, which are of great concern to the IDS users. More specifically, an IDS is of poor performance if it is high in false positive and false negative rate, for the reason that it is not effective in that case. False positive refers to the extent that IDS mistakenly consider a harmless event as an attack, for instance, an user operates within activity scope of what he is supposed to do and surprisingly, IDS detects his conduct as an attack and trigger an alarm followed by a response. On the contrary, a negligence that an attack which is supposed to be detected by IDS, however is erroneously considered as harmless means False Negative.

Based on the analysis method, IDS is classified into Anomaly Detection and Misuse Detection.

a. Anomaly Detection

When Anomaly Detection is performed, it is supposed to summarize beforehand what characteristics a normal operation has, that is called a profile in short. In other words, if a profile of a user is given, a set of its normal behaviors is established, as a result, behaviors significantly not conforming to its profile will be considered as an intrusion.

b. Misuse Detection

Misuse detection is a collection, opposite to anomaly detection, of the abnormal behaviors which are previously recorded and defined as misuse or attack behaviors for the establishment of a characteristic database. Therefore, a behavior, in accordance with the recording in the database, will be considered as an intrusion.

Note how anomaly detection and misuse detection work individually. The implementation of misuse detection is feature matching. A conclusion of an act as an attack is made based on how it behaves whether it matches with the how it recorded and defined in database, while anomaly detection is achieved by statistics, an intrusion will be considered an anomaly when the detected behaviors considerably deviated from the statistical figure. As a result, anomaly detection and misuse detection are two IDS types based on analysis.

2. Data source-based IDS

Based on the data source, there are two types: host-based IDS and network-based IDS.

a. Host-based IDS

Host-based IDS (abbreviated as HIDS): acquired data information(such as host system status, event logging, and so on) is taken from the host on which the IDS is operational. In other words, the IDS host is the source from which all the information originated, simultaneously, it is also the object under protection. For example, there are various servers (WWW server, Mail server) in the DMZ of the firewall, installation of HIDS on a host would be a protection of the servers.

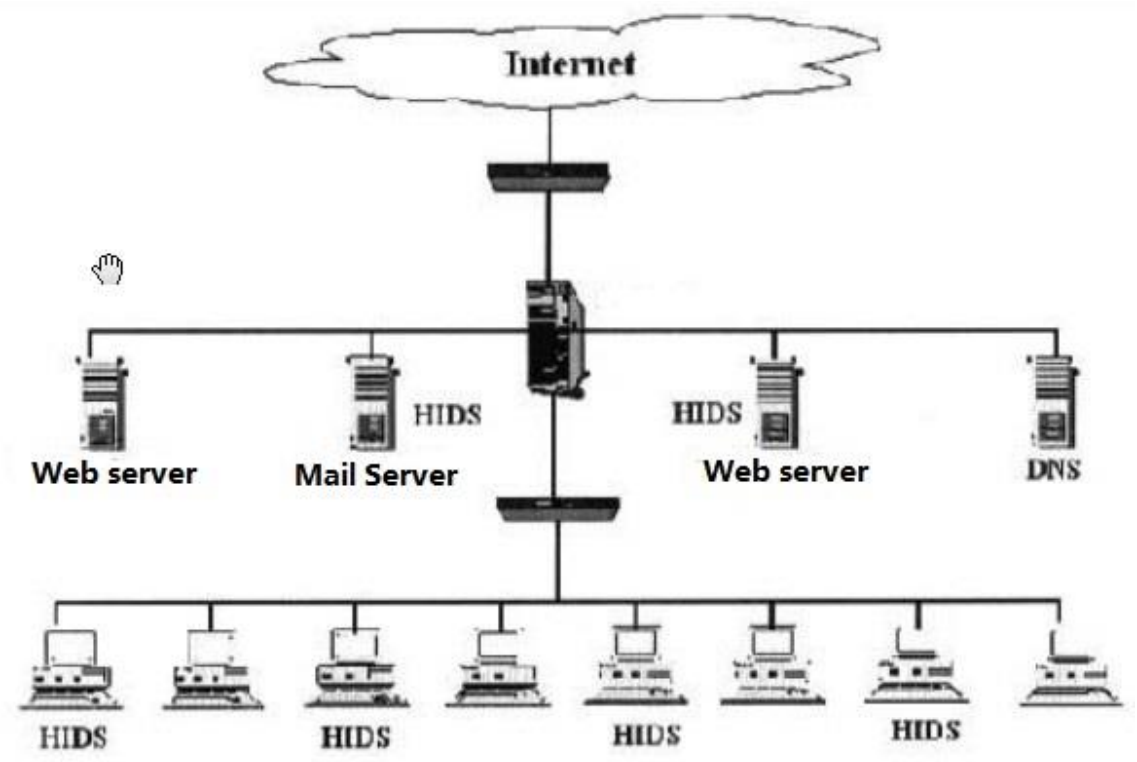

Figure 4.6 Example of a HIDS Deployment

(http://www.doc88.com/p-387499083772.html)

HIDS, taking advantage of the target host's audit records, application log, log files and so on for monitoring and analysis, mainly functions as a safeguard for the important application servers. Note that HIDS is excellent at detecting of the misuses resulting from the reliable internal staff carelessness or negligence, as well as, illegal activities successful in bypassing the traditional detection penetrate into the network. For example, intrusive packets, considered by the firewall as normal and unthreatening and forwarded into the internal network, can be detected on a specific host by HIDS. Two factors play an important role in determining how effective a HIDS would be, which are a timely collection of audit records and how to protect HIDS as an attacked target. For the first factor, during an intrusion, failing to collect part of or the whole of audit records, will result in a launched successful malicious operation on the host or system

before it is detected. As result, only a collection of audit record without delay will make a satisfactory monitoring. For the second factor, it is the hacker's awareness that important servers are installed with HISD, which, therefore become the most tempting target of the attacker.

b. Network-based IDS

For the network-based IDS, the data source collected by the event generator is packets transmitted through network with the intention to protect network and assure its daily normal operation.

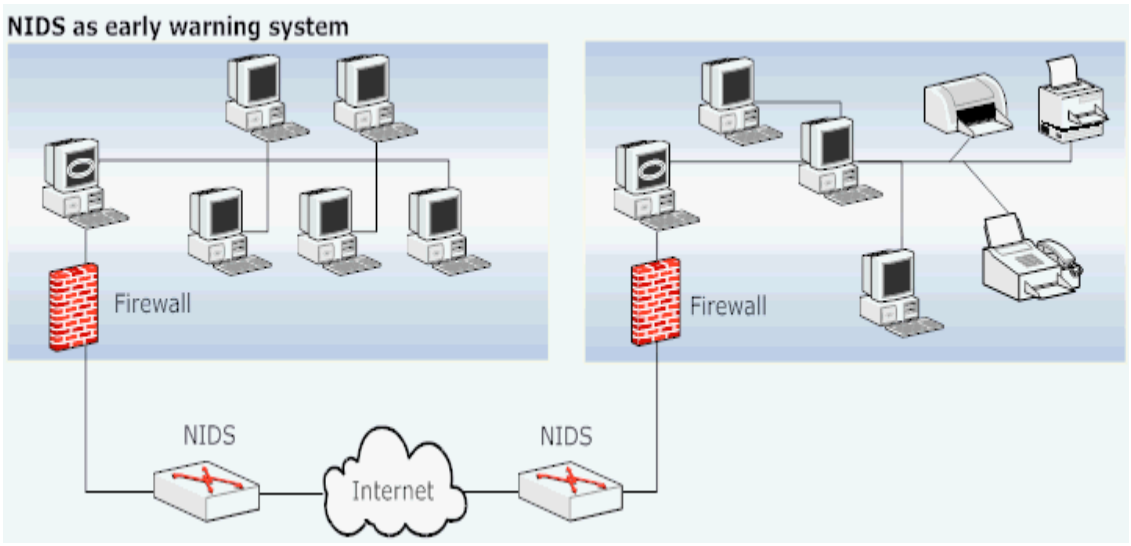

Figure 4.7 Example of a NIDS Deployment

(www.google.com.hk)

About the location of NDIS, rather than at the important servers, NDIS is deployed at the important points of the share network segment. In other words, installation of NIDS is made at a position at which is a network segment of vital importance and through which traffic transmitted needs to be monitored

NIDS lays its monitoring on the network traffic transmitted across detection agents located in shared network segments, through this process abnormal behaviors and attacks are detected after being analyzed. Because the installation is not on a host NIDS is low in host resource consumption (CPU, memory etc.). Besides, NIDS protects an important network segment by the means of installation of sensors.

5.4 IDS Approaches

Anomaly Detection Technique

Two IDS approaches based on anomaly detection principle are statistical anomaly detection and neural network-based anomaly detection.

1) Statistical Anomaly Detection

The statistical anomaly detection technique is an IDS approach which is the earliest and most frequently applied. The main idea of anomaly detection is to collect the legal users normal behaviors according to which, afterwards, their characteristic are defined and the corresponding database (profile) is built. What an user is currently doing will be recorded in his/her current profile. During the analysis process, a combination of what the same user did recorded in the history profile with the current profile constitutes an updated statistical profile. Later on, according to probability and statistics, by comparison the current profile with the statistical profile, a conclusion of whether abnormal behavior occurs or not will be made. Note the update of the statistical profile is, on a regular basis, a new integration of the history profile and current profile which becomes different as time goes on.

Statistical anomaly detection advantage:

Well-studied statistical theory is available to be applied for the mathematical work, such as comparisons with other models or mathematical proofing.

Statistical anomaly detection disadvantages:

a. A decision whether an user's behaviors is conform to its history profile is an act of considerable difficulty, as users behave in a diverse and complicated way. For a certain users' operations there is their history profile, but it is fairly difficult to summarize a complete set of the characteristic behaviors. Consequently, statistical anomaly detection, relying on user profile acquired by statistics results, tends to make false positives and false negatives when it is applied.

b. It is difficult to define the intrusion threshold. That is to say, how much the behavior's deviation from the profile is considered to be a normal and abnormal is very hard to define. As it can be imagined, a high threshold results in a high false positives while a low threshold causes a high false negatives in which attacks will be neglected.

2) Neural Network-Based Anomaly Detection

Neural network is a term often mentioned in the field of artificial intelligence, whose main idea is to train neurons by a series of information units and the focus is on the process of training. For anomaly detection, the key of the success is to accurately form a user normal daily characteristic profile. A neural network-based anomaly detection(abbreviated as NNAD) is able to extract what is the characteristic of an user's normal behaviors by self-study and training on provision of system audit data. From this process, a self-adaptive characteristic profile is formed, which remarkably assists in the NNAD's accurate reaction against the rare but within normal characteristic quantity behaviors, along with,

variants of unknown intrusions, therefore, making it low in false alarms rate and a consequential adaptation to the ever-changing network environments. What is more, there is no need for an additional room for the storage for database of the characteristic profile.

Before the discussion of a NNAD model, a brief introduction of Neural Network Classifier will be presented. Neural Network Classifier is designed for the analysis and process of the feature vector generated from the data flow. After, the data flow has been examined, it is concluded whether is normal or not. If it is an attack, the neural network classifier will issue an alarm and record it in its log. In the case that the reported attack is valuable for a better complete attack database , for instance a new attack which has never been detected before. The reported attack will be added into and be a part of the attack database for the further study by itself, therefore, the neural network classifier's capability of processing is increasing (Jingxin et al., 2003).

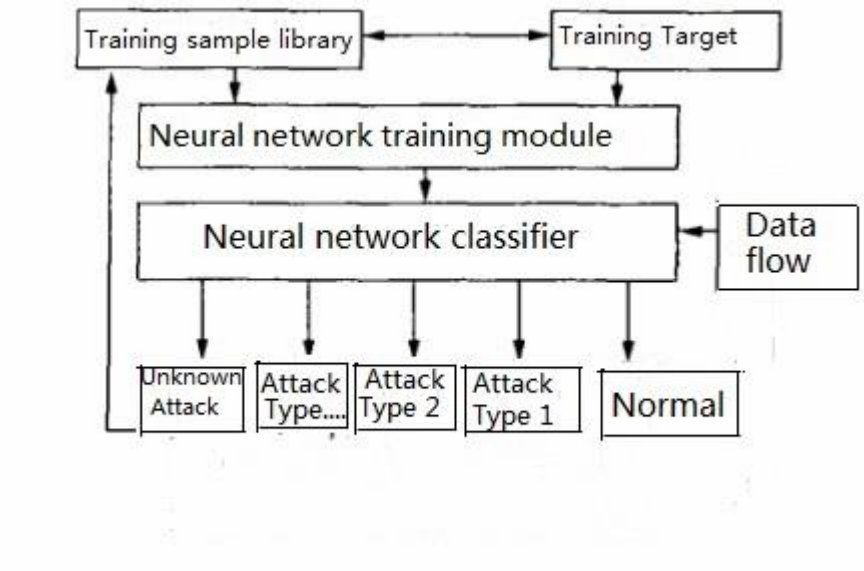

Figure 4.8 Example of a neural network-based anomaly detection model.

(http://www.doc88.com/p-1874786520150.html)

In neural network-based anomaly detection, the initial step is to acquire and study the traditional network attacks sample as its learning sample library, for the training of the neural network classifier. Afterwards, using weights, the neural network will store the characteristic model of these attacks, simultaneously, the neural network classifier start to function for the analysis and process of the captured network data flow, finally making a decision of whether it is normal nor malicious. If it is an unknown attack, it will be sent to the training sample library as a feedback. This is a demonstration of the neural network-based anomaly detection's ability in self-study and identification of unknown attacks (Jingxin et al., 2003).

Misuse Detection Technique

The misuse detection technique is applied on the assumption that attacks are precisely coded in a certain way, actually, the characteristic of every attack is extractable, which can be captured and determined by an intrusion variant based on the same vulnerability. For instance, many attacks share the same characteristic, of which minor changes are made but its feature remains the same as before, as a result, it has no effect on confusing misuse detection and detectable.

The definition of misuse detection: intrusion detection is implemented by model matching based on the pre-defined intrusion model and what is observed during an intrusion. An intrusion model, composed of certain predefined intrusion models and their extracted characteristic, holds the conditions, order, essential features and so on of the intrusion, all of which are used for the matching of an intrusion. An incomplete intrusion model might be a representation of an intrusion constructed in multiple ways. In other words, that is called an variance of intrusion and is launched in a different way based on the same vulnerability.

Common misuse detections are expert system misuse detection and state transition analysis misuse detection.

5.5 Expert System misuse Detection

Currently, expert system misuse detection is the most widely applied detection technique, as the term might indicate, whose main idea is to express the security expert's knowledge in the structure of If-Then. Conditions required for the intrusion make up the "if" section, while the "then" section is the corresponding countermeasure to be taken against the intrusion. Expert knowledge base, a container of all the if-then structures, with which inference engine draws conclusion of intrusion detection.

For example, provided the assumption that if the source IP address is the same as the destination IP address, then it is DOS attack and action for defense is taken. As can be seen that the first judgment will determine whether the condition fits as predefined, if yes then it provides method to respond to it. In other words, a predefined item (if source IP address is the same as the destination IP address) is stored in the expert knowledge base, and then the related defense is to filter and drop the packets initiated from that host. Thus, the if-then rule structure is built.

Note two main problems which are the processing of sequence data and the maintenance of the knowledge base when applying expert system analysis misuse detection. Especially the knowledge base maintenance on which the decision how to respond and react is based when intrusion is detected, thus, the update and maintenance is undoubtedly important. Failure to update the knowledge base will result in incapability of new intrusion detection. Even a frequent timely update and maintenance will not be a guarantee of detecting all

intrusions, more precisely, limit to only known attacks, for the reason that there is no way for the summarization of the characteristics of unknown attacks. As a result, knowledge acquisition poses an obstacle to a robust expert system misuse detection.

5.6 State Transition Analysis Misuse Detection

Essentially, state transition analysis is a rule-based misuse detection which is represented by stat transition diagram and used for detection of known attack model. The implementation is that the whole intrusion process is considered to be a change-of-state model, constructed by a series of attacker's actions which causes the system to change from its initial secure state to be compromised.

The state referred above means the description of computer system at specific moments. There are three states about the system as follows:

a. Initial state: also referred as secure state is a state when communications between network are normal and legal prior to intrusion.

b. Transit state: a state which is under attack .

c. Intrusion state: a state when the network has already been compromised by the intrusion.

The state transition diagram is a representation of a series of crucial actions which makes, after transit state(s), the system change from the initial state to intrusion state. State transit analysis is an approach demonstrating the action sequence of the intrusion from the beginning to its final success provided the changing states of the computer system can be monitored as the changing state of a launched intrusion, in the case, which can also be detectable. The information of the system state is diverse and various such as temporary or permanent value of memory address, username, process ID and so on. As for the state transit diagram's representation of a certain intrusion, not all but only the information is required for presenting change from initial state to transit state and then intrusion state. For the implementation of state transit analysis, a mechanism which records the changing state of the system property is required. That is a computer system built audit record and monitor tool which keeps record of changing state of detection system property. Then, the necessary information acquired from the audit record as input, which, by the designed analysis tool, compares the changing state with the known intrusion state transition diagram to reach conclusion (Shuang 2005).

6. Summary

The thesis first presents the characteristics and current situation of the network, including the common network attacks we encounter, analysis of the diverse threats originated from Internet. Afterwards introduces the specific intrusions

technologies and knowledge and factors that might have an impact on the network security. To be concluded, factors are: inherent defects and vulnerabilities of the network protocols and network devices, staff mal-administration, new hacking methods are introduced, improper design of the network models, users insufficient awareness of information security and so on. The discussions of the intrusions are examined also from the perspective of the attackers. For example necessary information is supposed to be gained as preparation for intrusion, what would be the vulnerable network devices and facilities would be an easy breaking point for intrusion etc. For these common network attacks, which pose a great threat to the network, the suggested corresponding countermeasures are provided respectively.

After the discussions of the common network threats, the thesis moves to two widely applied defense technologies firewall and intrusion detection system. According to the different needs of customers, the functions and models of the firewall vary from one to another. Generally speaking, as an important means of network security measure, a firewall mainly serves as a prevention of the unauthorized user's access into internal network as well as to sensitive data, simultaneously, as a filter of unsecure service, allowing legal user's visit to network resource without any restriction. However, there are limitations of the firewall, for example, a firewall is neither effectively functional in guarding against the inner attacks, nor, its capability effective in scanning and detecting every single infected software or file while transmission. As conclusion, there exists no once-for-all defense technology. A wise combination of different technologies would be an integrated and coordinated network security defense structure. Intrusion Detection System (IDS), which is a dynamic and active defense, would be a proper complement to the firewall technology. IDS serves as an analyzer and detector of the illegal activities which might be a potential threat to the security, by monitoring the incidents happen in the computer or network. In details, IDS sets certain key points in the computer network and system for information collection, from which to determine if there are any signs of being attacked or activities against the security strategies implemented made by the administrators, afterwards, take timely and appropriate response as countermeasures based on the analysis.

As a conclusion, firewall technology and IDS are complementary to each other. IDS's advantages in timely, fast and dynamic assist the firewall's function in its packet-filtering and access control. A combination of these two technologies will be an significant increase in the network security.

References

Xiongyue, L., 2011. "Network Information Security Situation"

http://www.docin.com/p-425600283.html,. Accessed 06th June, 2013.

Krawetz, N., 2006. “Introduction to Network Security”, Boston, MA, USA: Charles River Media Press.

2012, “SYN Flood Theory and Defense”,

http://blog.sina.com.cn/s/blog_4129523901013uuj.html Accessed 20th April, 2013.

Blank, A.G., 2002. “Internet Protocol Basics”. Alameda, CA, USA: Sybex Press.

Akshaya, B., & Katebarry, 2008. “Man-in-the-Middle Attack”,

http://it.toolbox.com/wiki/index.php/Man-in-the-Middle_Attack Accessed 22nd April, 2013.

Ye, N., 2008. “Secure Computer and Network System: Modeling, Analysis and Design”. Chichester, Great Britain: John Wiley & Sons, Ltd.

Vivek, R., & Sukumar, N., 2013. “Detecting ARP Spoofing: An Active Technique”

http://wenku.baidu.com/view/93ac1cb7960590c69ec37689.html

Accessed 25th April, 2013.

Preetham, V., 2002. “Internet Security and Firewalls”. Boston, MA, USA: Course Technology Press.

Dapeng, J., 2006. “Research and Implementation of Data Selection Model in Intrusion Detection System” Master’s Thesis,

http://www.doc88.com/p-1761662624426.html Accessed 18th May, 2013.

Jingxin, W., Hui, D., Hui, S., & Zhiying, W., 2003. “An Intrusion Detection System Based on Artificial Neural Network”

http://www.doc88.com/p-1874786520150.html Accessed 02nd June, 2013.

Shuang, Zheng., 2005 “Study and Design on state transition-based intrusion detection analysis engine” Bachelor’s thesis

http://www.doc88.com/p-0641669527097.html Accessed 05th June, 2013.

Rey, M. D., 1981. “Internet Protocol DARPA Internet Program Protocol Specification”,

http://www.networksorcery.com/enp/rfc/rfc791.txt Accessed 26th, August, 2013.

Russ, R., Miles, G., Ed, Fuller., Ted, D., & Matthew, H., December, 2003. “Security Assessment: Case Studies for Implementing the NSA Iam”, Rockland, MA, USA: Syngress Publishing.